

# Информационная безопасность

## Л.5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ширяев Кирилл Владимирович

2021

### Содержание

Цель работы .....	2
Подготовка лабораторного стенда .....	2
Компилятор gcc .....	<b>Ошибка! Закладка не определена.</b>
Система запретов .....	<b>Ошибка! Закладка не определена.</b>
Ход работы .....	2
Программа simpleid.c .....	2
Компиляция simpleid.c .....	3
Выполнение simpleid.c и id .....	4
Программа simpleid2.c .....	5
Компиляция и выполнение simpleid2.c .....	6
Смена владельца и атрибут s .....	7
Запуск simpleid2 с SetUID .....	8
Запуск simpleid2 с SetGID .....	<b>Ошибка! Закладка не определена.</b>
Программа readfile.c .....	9
Компиляция и изменение readfile.c .....	10
Изменение владельца readfile с SetUID .....	<b>Ошибка! Закладка не определена.</b>
Попытка прочтения .....	<b>Ошибка! Закладка не определена.</b>
Атрибут Sticky на /tmp .....	11
Создание file01.txt .....	12
Атрибуты file01.txt .....	13
Работа с файлом file01.txt в директории с t .....	14
Снятие атрибута t .....	15
Работа с файлом file01.txt в директории без t .....	16
Возврат атрибута t .....	17
Вывод .....	18

## 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.

## Подготовка лабораторного стенда

## Ход работы

### Программа simpleid.c

Вошли в систему от имени пользователя guest и создали программу simpleid.c:

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[kvshiryaev@kvshiryaev ~]$ pwd
/home/kvshiryaev
[kvshiryaev@kvshiryaev ~]$ touch simplified.c
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
```

```
kvshiryaev@kvshiryaev:~
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.9.8      simplified.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;
}
```

[ Read 12 lines ]

<b>^G</b> Помощь	<b>^O</b> Записать	<b>^W</b> Поиск	<b>^K</b> Вырезать	<b>^J</b> Выводить	<b>^C</b> ТекПозиц
<b>^X</b> Выход	<b>^R</b> ЧитФайл	<b>^_</b> Замена	<b>^U</b> Отмен. выр	<b>^T</b> Словарь	<b>^</b> К строке

Figure 3: Программа `simplified.c`

### Компиляция `simplified.c`

Скомпилировали программу и убедились, что файл программы создан:

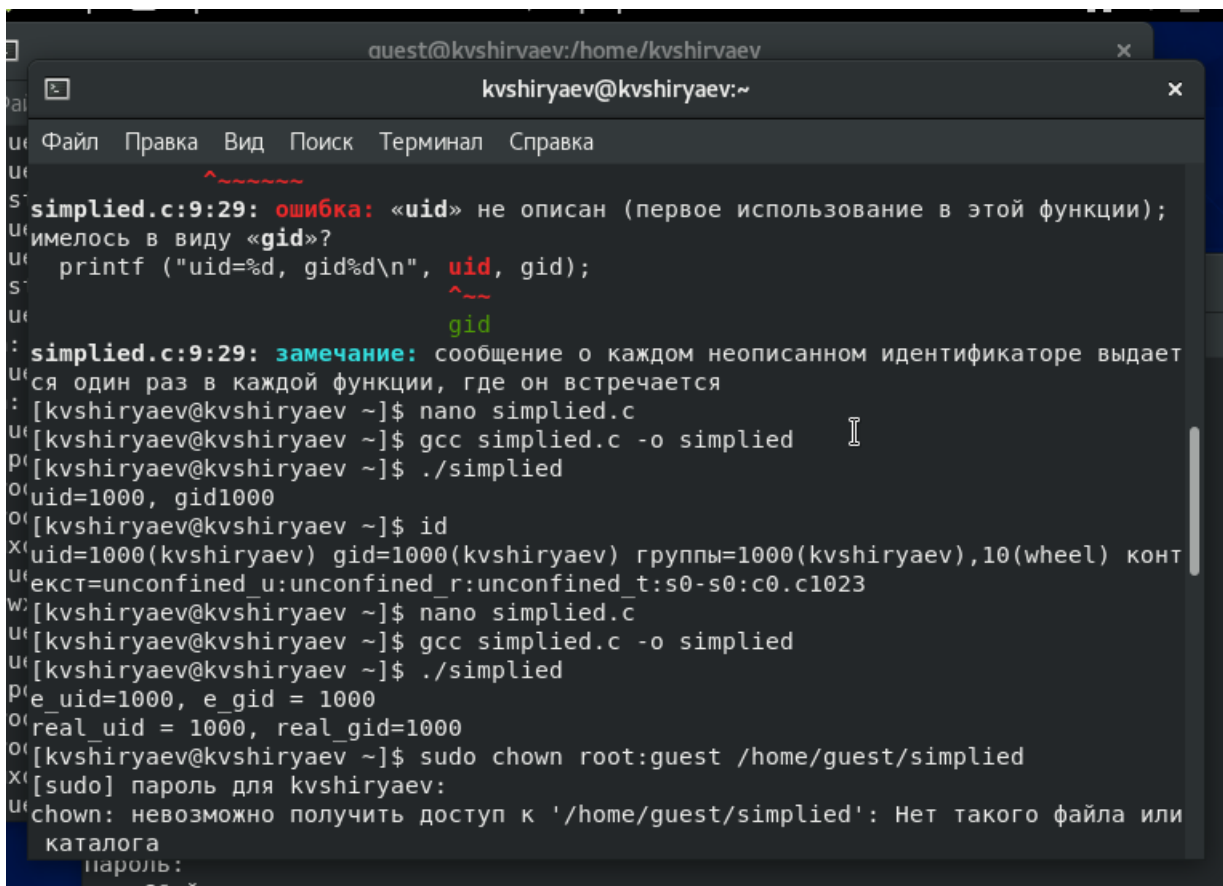
```
gcc simplified.c -o simpleid
```

```
quest@kvshiryaev:/home/kvshiryaev
kvshiryaev@kvshiryaev:~
Файл Правка Вид Поиск Терминал Справка
~~~~~
simplified.c:9:29: ошибка: «uid» не описан (первое использование в этой функции);
имелось в виду «gid»?
printf ("uid=%d, gid%d\n", uid, gid);
                        ^~~
                        gid
: simplified.c:9:29: замечание: сообщение о каждом неопisanном идентификаторе выдает
ся один раз в каждой функции, где он встречается
: [kvshiryaev@kvshiryaev ~]$ nano simplified.c
: [kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
: [kvshiryaev@kvshiryaev ~]$ ./simplified
o uid=1000, gid1000
o [kvshiryaev@kvshiryaev ~]$ id
x uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) конт
eкст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
w [kvshiryaev@kvshiryaev ~]$ nano simplified.c
u [kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
u [kvshiryaev@kvshiryaev ~]$ ./simplified
p e_uid=1000, e_gid = 1000
o real_uid = 1000, real_gid=1000
o [kvshiryaev@kvshiryaev ~]$ sudo chown root:guest /home/guest/simplified
x [sudo] пароль для kvshiryaev:
u chown: невозможно получить доступ к '/home/guest/simplified': Нет такого файла или
каталога
пароль:
... Сбой при проверке привилегий
```

Figure 4: Компиляция `simpleid.c`

## Выполнение `simpleid.c` и `id`

Выполнили программу `simpleid`: `./simpleid`, а также системную программу `id`:



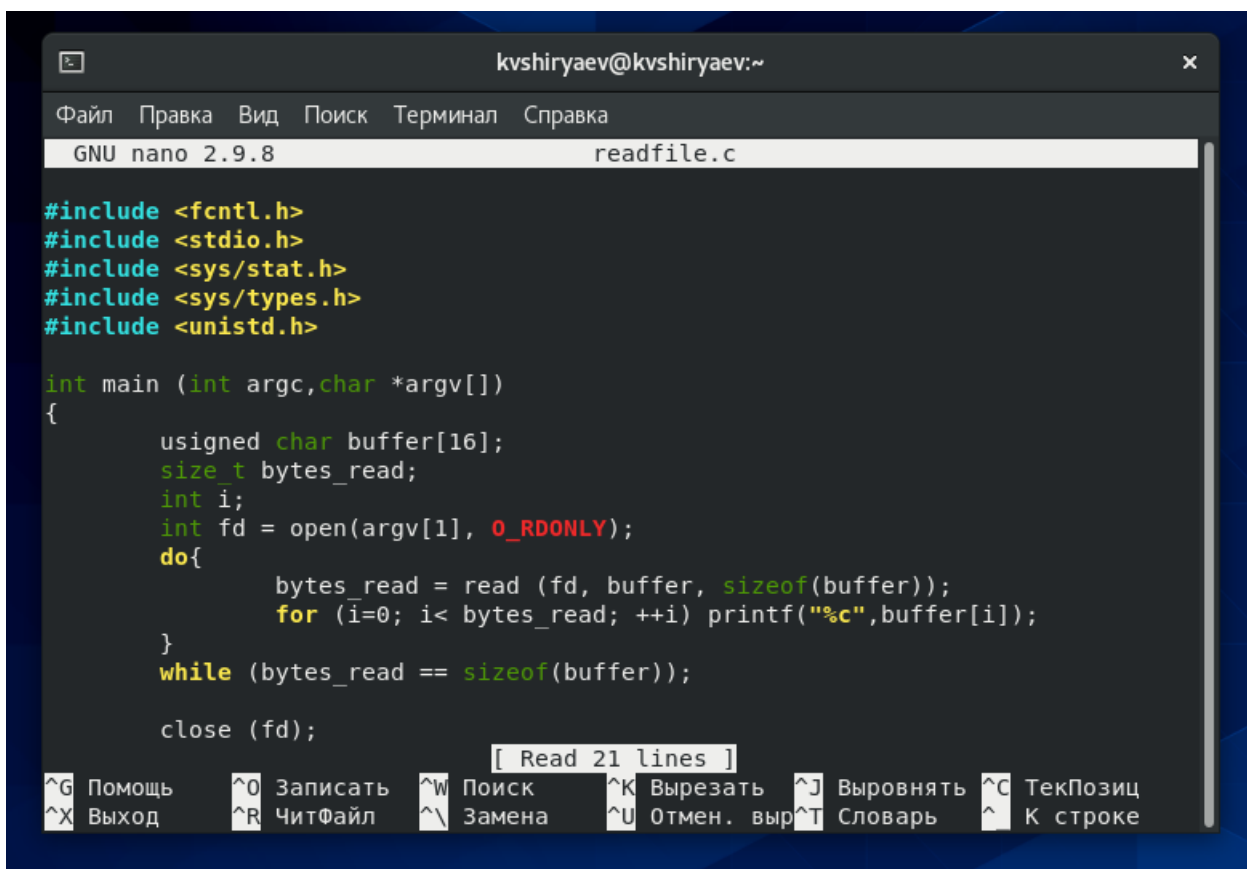
```
quest@kvshiryaev:/home/kvshiryaev
kvshiryaev@kvshiryaev:~
Файл  Правка  Вид  Поиск  Терминал  Справка
~~~~~
simplified.c:9:29: ошибка: «uid» не описан (первое использование в этой функции);
имелось в виду «gid»?
printf ("uid=%d, gid%d\n", uid, gid);
                        ^~~
                        gid
: simplified.c:9:29: замечание: сообщение о каждом неопisanном идентификаторе выдает
ся один раз в каждой функции, где он встречается
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
[kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
[kvshiryaev@kvshiryaev ~]$ ./simplified
uid=1000, gid=1000
[kvshiryaev@kvshiryaev ~]$ id
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) конт
екст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
[kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
[kvshiryaev@kvshiryaev ~]$ ./simplified
e_uid=1000, e_gid = 1000
real_uid = 1000, real_gid=1000
[kvshiryaev@kvshiryaev ~]$ sudo chown root:guest /home/guest/simplified
[sudo] пароль для kvshiryaev:
chown: невозможно получить доступ к '/home/guest/simplified': Нет такого файла или
каталога
пароль:
Сбой при проверке разрешения
```

Figure 5: Выполнение `simplified.c` и `id`

Получили идентичные результаты рассматриваемых параметров

## Программа `simpleid2.c`

Усложнили программу, добавив вывод действительных идентификаторов, и назвали её `simpleid2.c`:



```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
GNU nano 2.9.8 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);  
}
```

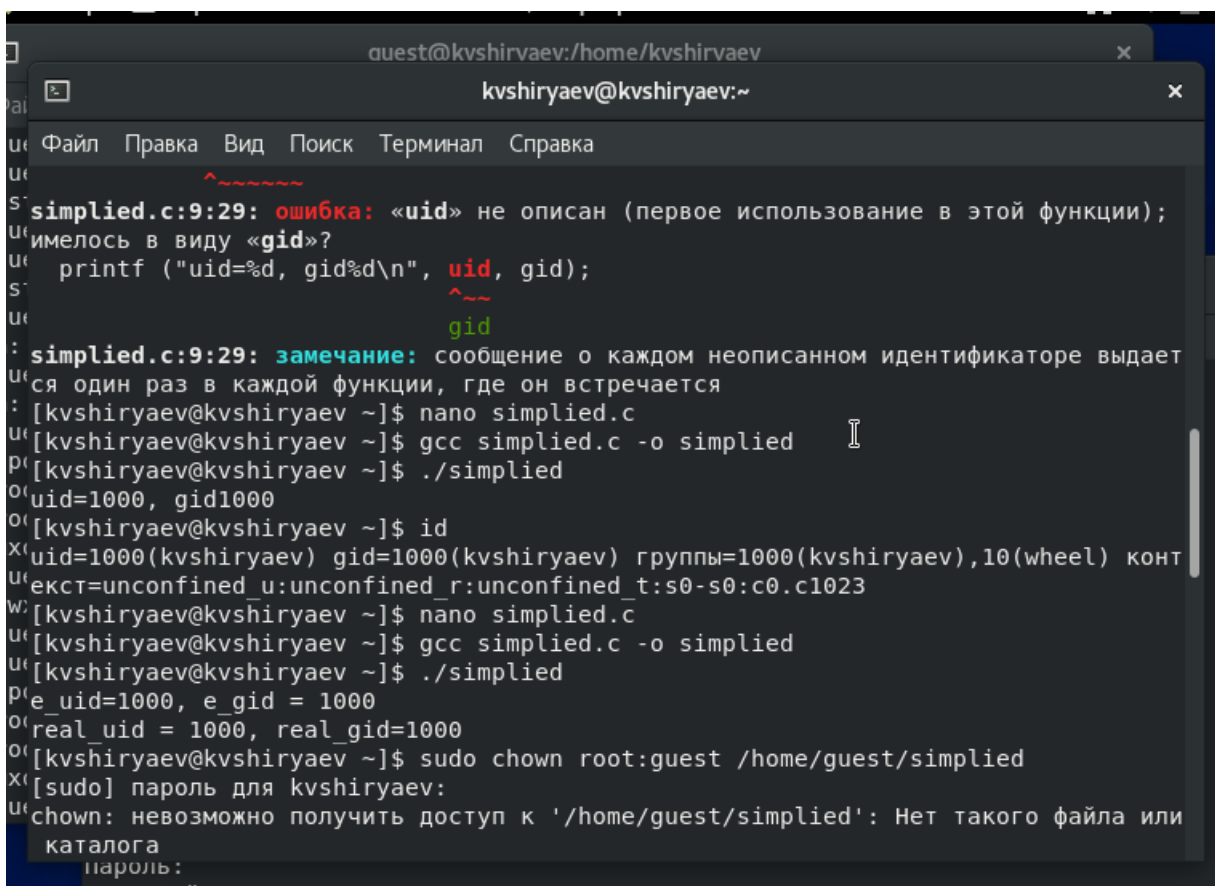
[ Read 21 lines ]

<b>^G</b> Помощь	<b>^O</b> Записать	<b>^W</b> Поиск	<b>^K</b> Вырезать	<b>^J</b> Выводить	<b>^C</b> ТекПозиц
<b>^X</b> Выход	<b>^R</b> ЧитФайл	<b>^_\</b> Замена	<b>^U</b> Отмен. выр	<b>^T</b> Словарь	<b>^</b> К строке

Figure 6: Программа simpleid2.c

## Компиляция и выполнение simpleid2.c

Скомпилировали и запустили программу simpleid2.c:



```
quest@kvshiryaev:/home/kvshiryaev
kvshiryaev@kvshiryaev:~
Файл  Правка  Вид  Поиск  Терминал  Справка
~~~~~
simplified.c:9:29: ошибка: «uid» не описан (первое использование в этой функции);
имелось в виду «gid»?
printf ("uid=%d, gid%d\n", uid, gid);
                             ^~~
                             gid
: simplified.c:9:29: замечание: сообщение о каждом неопisanном идентификаторе выдает
ся один раз в каждой функции, где он встречается
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
[kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
[kvshiryaev@kvshiryaev ~]$ ./simplified
uid=1000, gid=1000
[kvshiryaev@kvshiryaev ~]$ id
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) конт
екст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[kvshiryaev@kvshiryaev ~]$ nano simplified.c
[kvshiryaev@kvshiryaev ~]$ gcc simplified.c -o simplified
[kvshiryaev@kvshiryaev ~]$ ./simplified
e_uid=1000, e_gid = 1000
real_uid = 1000, real_gid=1000
[kvshiryaev@kvshiryaev ~]$ sudo chown root:guest /home/guest/simplified
[sudo] пароль для kvshiryaev:
chown: невозможно получить доступ к '/home/guest/simplified': Нет такого файла или
каталога
пароль:
Сбой при проверке привилегий
```

Figure 7: Компиляция и выполнение `simpleid2.c`

Теперь видим не только текущих группу и пользователя, но и владельца файла.

## Смена владельца и атрибут `s`

От имени суперпользователя выполнили команды:

```
chown root:guest /home/guest/simpleid2
```

```
chmod u+s /home/guest/simpleid2
```

Тем самым, сменили владельца файла и добавили ему дополнительный атрибут (SetUID).

Затем выполнили проверку правильности установки новых атрибутов и смены владельца файла `simpleid2`:

```
ls -l simpleid2
```

```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
e_uid=1000, e_gid = 1000  
real_uid = 1000, real_gid=1000  
[kvshiryaev@kvshiryaev ~]$ sudo chown root:guest /home/guest/simplified  
[sudo] пароль для kvshiryaev:  
chown: невозможно получить доступ к '/home/guest/simplified': Нет такого файла или каталога  
[kvshiryaev@kvshiryaev ~]$ su root  
Пароль:  
[root@kvshiryaev kvshiryaev]# sudo chown root:kvshiryaev /home/kvshiryaev/simplified  
[root@kvshiryaev kvshiryaev]# chmod u+s /home/kvshiryaev/simplified  
[root@kvshiryaev kvshiryaev]# ls -l simplified  
-rwsrwxr-x. 1 root kvshiryaev 17744 фев 22 13:14 simplified  
[root@kvshiryaev kvshiryaev]# ./dimplied  
bash: ./dimplied: Нет такого файла или каталога  
[root@kvshiryaev kvshiryaev]# ./simplified  
e_uid=0, e_gid = 0  
real_uid = 0, real_gid=0  
[root@kvshiryaev kvshiryaev]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@kvshiryaev kvshiryaev]# su kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ pwd  
/home/kvshiryaev  
пароль:  
Сбой при проверке подлинности
```

Figure 8: Смена владельца и атрибутов

## Запуск simpleid2 с SetUID

Запустили simpleid2 и id, вновь получили идентичные результаты.

Убедились в принадлежности файла пользователю root.

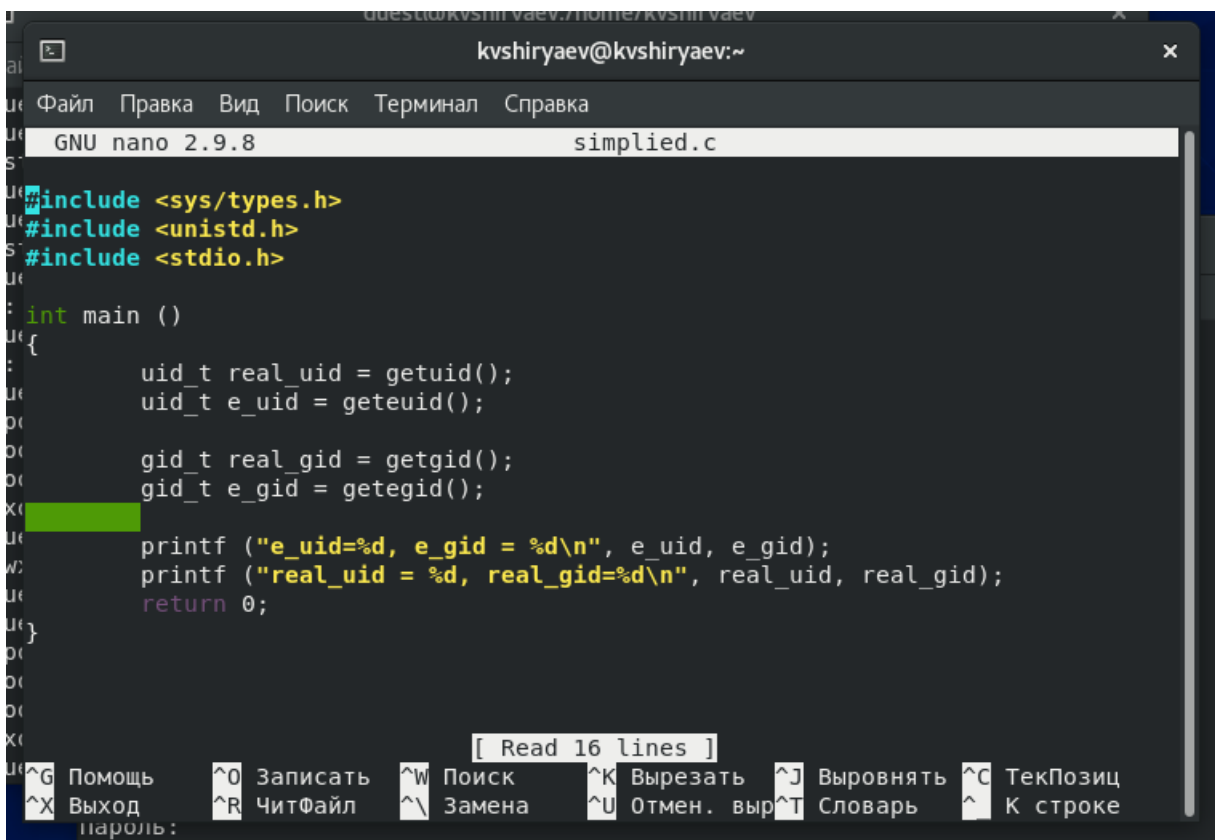


```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
e_uid=1000, e_gid = 1000  
real_uid = 1000, real_gid=1000  
[kvshiryaev@kvshiryaev ~]$ sudo chown root:guest /home/guest/simplified  
[sudo] пароль для kvshiryaev:  
chown: невозможно получить доступ к '/home/guest/simplified': Нет такого файла или каталога  
[kvshiryaev@kvshiryaev ~]$ su root  
Пароль:  
[root@kvshiryaev kvshiryaev]# sudo chown root:kvshiryaev /home/kvshiryaev/simplified  
[root@kvshiryaev kvshiryaev]# chmod u+s /home/kvshiryaev/simplified  
[root@kvshiryaev kvshiryaev]# ls -l simplified  
-rwsrwxr-x. 1 root kvshiryaev 17744 фев 22 13:14 simplified  
[root@kvshiryaev kvshiryaev]# ./dimplied  
bash: ./dimplied: Нет такого файла или каталога  
[root@kvshiryaev kvshiryaev]# ./simplified  
e_uid=0, e_gid = 0  
real_uid = 0, real_gid=0  
[root@kvshiryaev kvshiryaev]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@kvshiryaev kvshiryaev]# su kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ pwd  
/home/kvshiryaev  
пароль:  
Сбой при проверке подлинности
```

Figure 9: Запуск simpleid2 с SetUID

## Программа readfile.c

Создали программу readfile.c:



```
kvshiryaev@kvshiryaev:~
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.9.8      simplified.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;
}

[ Read 16 lines ]
^G  Помощь  ^O  Записать  ^W  Поиск      ^K  Вырезать  ^J  Выводить  ^C  ТекПозиц
^X  Выход    ^R  ЧитФайл   ^\  Замена     ^U  Отмен. выр ^T  Словарь   ^_  К строке
пароль:
```

Figure 11: Программа readfile.c

### Компиляция и изменение readfile.c

Откомпилировали программу и изменили владельца у файла readfile.c и права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог, убедились в правильности, получив отказ в доступе:

```
quest@kvshiryaev:/home/kvshiryaev
kvshiryaev@kvshiryaev:~
Файл Правка Вид Поиск Терминал Справка
[kvshiryaev@kvshiryaev ~]$ touch readfile.c
[kvshiryaev@kvshiryaev ~]$ nano readfile.c
[kvshiryaev@kvshiryaev ~]$ nano readfile.c
[kvshiryaev@kvshiryaev ~]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:9:2: ошибка: «unsigned» не описан (первое использование в этой функции
)
    unsigned char buffer[16];
    ^~~~~~
readfile.c:9:2: замечание: сообщение о каждом неопisanном идентификаторе выдается
одн раз в каждой функции, где он встречается
readfile.c:9:9: ошибка: expected «;» before «char»
    unsigned char buffer[16];
    ^~~~~~
;
readfile.c:14:26: ошибка: «buffer» не описан (первое использование в этой функци
и); имелось в виду «setbuffer»?
    bytes_read = read (fd, buffer, sizeof(buffer));
                        ^~~~~~
                        setbuffer
[kvshiryaev@kvshiryaev ~]$ nano readfile.c
[kvshiryaev@kvshiryaev ~]$ nano readfile.c
[kvshiryaev@kvshiryaev ~]$ gcc readfile.c -o readfile
[kvshiryaev@kvshiryaev ~]$
```

Figure 12: Компиляция и изменение readfile.c

## Атрибут Sticky на /tmp

Выяснили, что на директории /tmp установлен атрибут Sticky:

```
ls -l / | grep tmp
```

```
guest2@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
[kvshiryaev@kvshiryaev ~]$ ls -l / grep tmp  
ls: невозможно получить доступ к 'grep': Нет такого файла или каталога  
ls: невозможно получить доступ к 'tmp': Нет такого файла или каталога  
/:  
итого 24  
lrwxrwxrwx. 1 root root 7 июн 22 2021 bin -> usr/bin  
dr-xr-xr-x. 5 root root 4096 фев 22 12:10 boot  
drwxr-xr-x. 20 root root 3120 фев 22 11:53 dev  
drwxr-xr-x. 150 root root 8192 фев 22 12:36 etc  
drwxr-xr-x. 6 root root 64 фев 22 12:31 home  
lrwxrwxrwx. 1 root root 7 июн 22 2021 lib -> usr/lib  
lrwxrwxrwx. 1 root root 9 июн 22 2021 lib64 -> usr/lib64  
drwxr-xr-x. 2 root root 6 июн 22 2021 media  
drwxr-xr-x. 2 root root 6 июн 22 2021 mnt  
drwxr-xr-x. 2 root root 6 июн 22 2021 opt  
dr-xr-xr-x. 216 root root 0 фев 22 11:53 proc  
dr-xr-x---. 6 root root 239 фев 22 13:15 root  
drwxr-xr-x. 44 root root 1220 фев 22 12:10 run  
lrwxrwxrwx. 1 root root 8 июн 22 2021 sbin -> usr/sbin  
drwxr-xr-x. 2 root root 6 июн 22 2021 srv  
dr-xr-xr-x. 13 root root 0 фев 22 11:53 sys  
drwxrwxrwt. 17 root root 4096 фев 22 13:23 tmp  
drwxr-xr-x. 13 root root 158 фев 22 09:56 usr  
drwxr-xr-x. 21 root root 4096 фев 22 10:06 var
```

Figure 15: Атрибут Sticky на /tmp

### Создание file01.txt

От имени пользователя guest создали файл file01.txt в директории /tmp со словом test:

```
echo "test" > /tmp/file01.txt
```

```
guest2@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
su: Сбой при проверке подлинности  
[kvshiryaev@kvshiryaev ~]$ su guest2  
Пароль:  
su: Сбой при проверке подлинности  
[kvshiryaev@kvshiryaev ~]$ su guest2  
Пароль:  
[guest2@kvshiryaev kvshiryaev]$ mdw  
bash: mdw: команда не найдена...  
[guest2@kvshiryaev kvshiryaev]$ pwd  
/home/kvshiryaev  
[guest2@kvshiryaev kvshiryaev]$ cd ~  
[guest2@kvshiryaev ~]$ pwd  
/home/guest2  
[guest2@kvshiryaev ~]$ echo "test" > /tmp/file01.txt  
bash: /tmp: Это каталог  
[guest2@kvshiryaev ~]$ echo "test" > /tmp/file01.txt  
[guest2@kvshiryaev ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt  
[guest2@kvshiryaev ~]$ chmod o+rw /tmp/file01.txt  
[guest2@kvshiryaev ~]$ ;s -; /tmp/file01.txt  
bash: синтаксическая ошибка рядом с неожиданным маркером «;»  
[guest2@kvshiryaev ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt  
[guest2@kvshiryaev ~]$
```

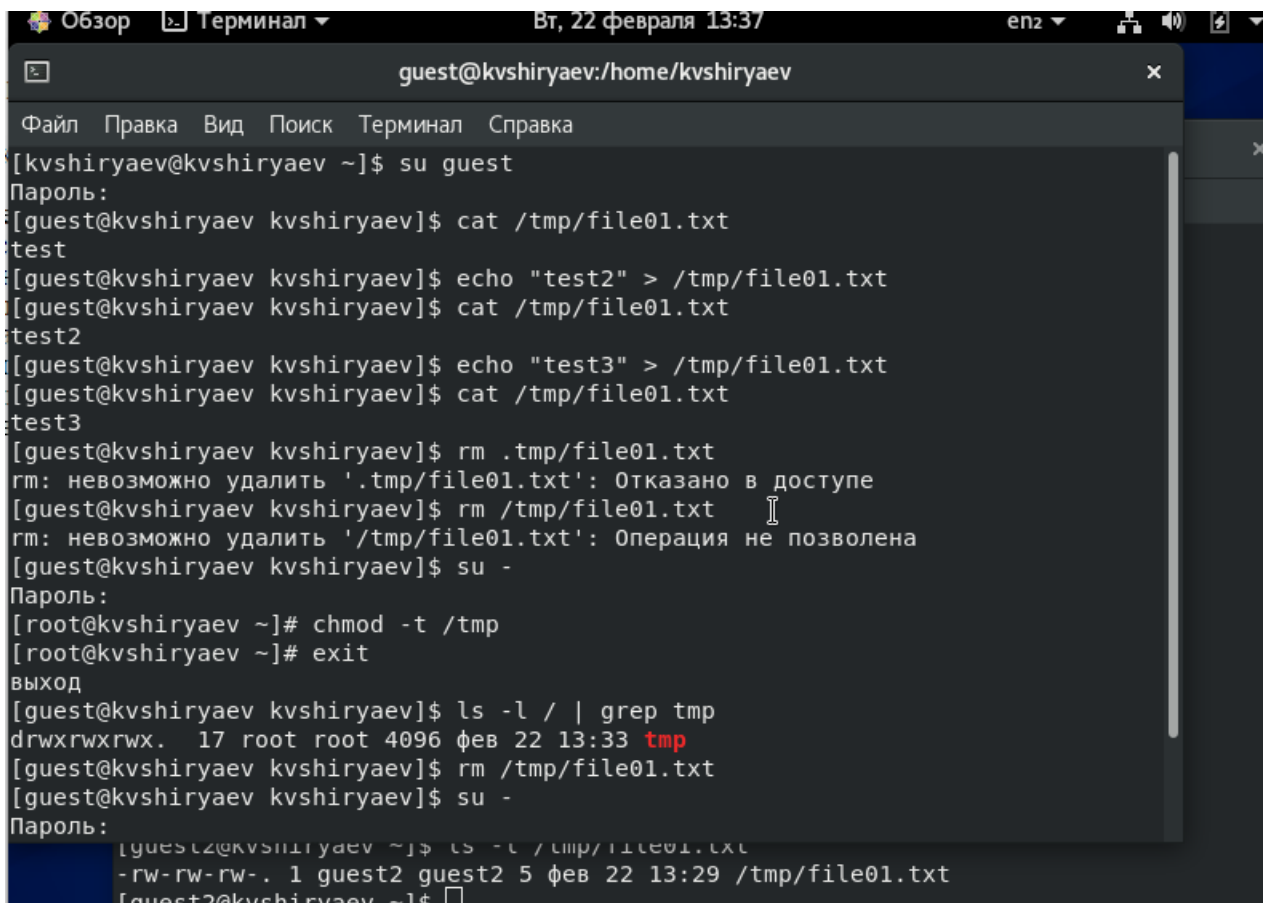
Figure 16: Создание file01.txt

### Атрибуты file01.txt

Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»:

```
chmod o+rw /tmp/file01.txt
```

```
ls -l /tmp/file01.txt
```



```
Обзор Терминал Вт, 22 февраля 13:37 en2
guest@kvshiryaev:/home/kvshiryaev
Файл Правка Вид Поиск Терминал Справка
[kvshiryaev@kvshiryaev ~]$ su guest
Пароль:
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test
[guest@kvshiryaev kvshiryaev]$ echo "test2" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test2
[guest@kvshiryaev kvshiryaev]$ echo "test3" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test3
[guest@kvshiryaev kvshiryaev]$ rm .tmp/file01.txt
rm: невозможно удалить './tmp/file01.txt': Отказано в доступе
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod -t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 фев 22 13:33 tmp
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[guest2@kvshiryaev ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt
[guest2@kvshiryaev ~]$
```

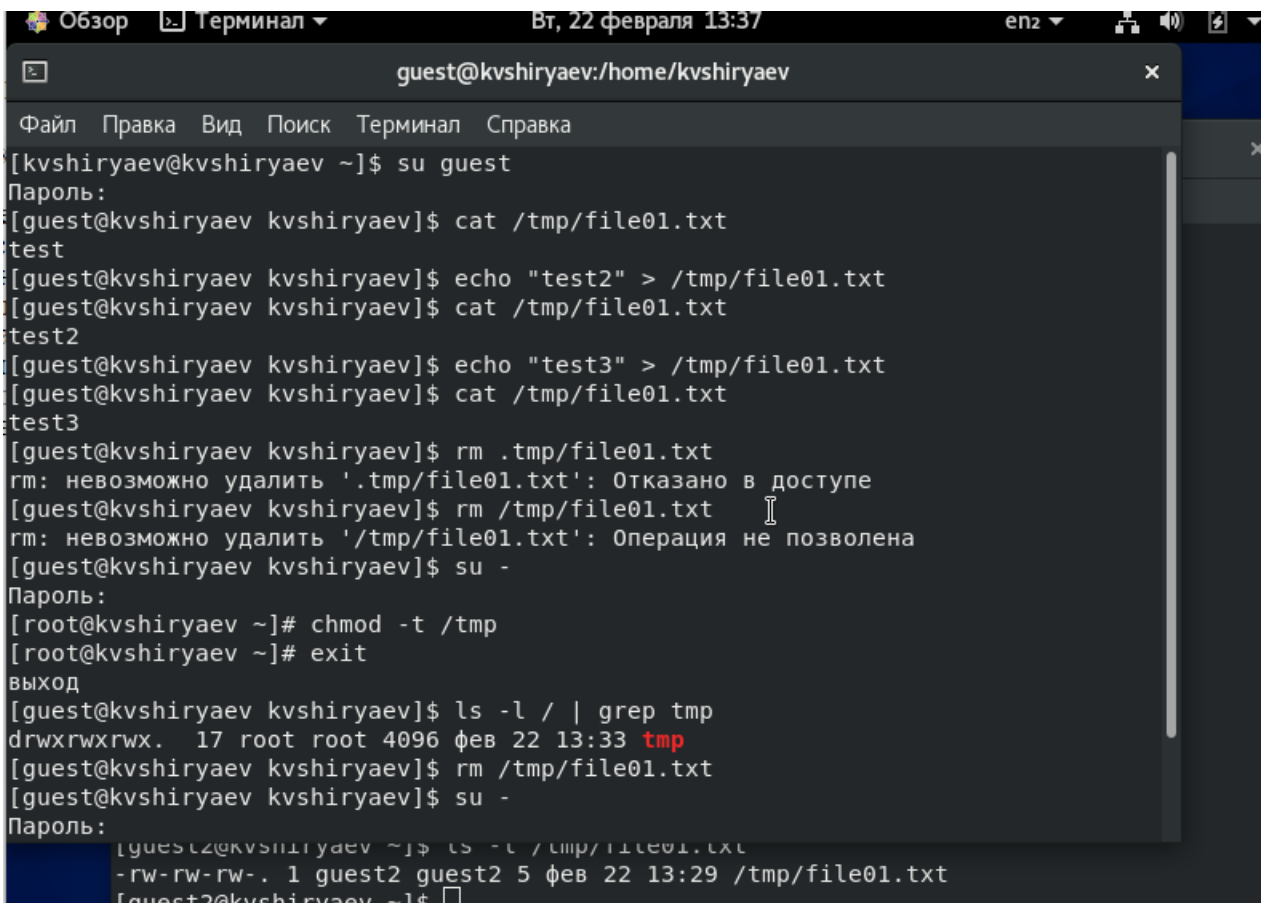
Figure 17: Атрибуты file01.txt

## Работа с файлом file01.txt в директории с t

От пользователя guest2 (не являющегося владельцем) попробовали:

1. прочитать файл /tmp/file01.txt: `cat /tmp/file01.txt`
2. дозаписать в файл /tmp/file01.txt слово test2: `echo "test2" >> /tmp/file01.txt`
3. проверить содержимое файла: `cat /tmp/file01.txt`
4. записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию: `echo "test3" > /tmp/file01.txt`
5. проверить содержимое файла: `cat /tmp/file01.txt`
6. удалить файл /tmp/file01.txt: `rm /tmp/file01.txt`

Удалось дозаписать информацию в файл, перезаписать, прочитать, но не удалось удалить файл:



```
Обзор Терминал Вт, 22 февраля 13:37 en2
guest@kvshiryaev:/home/kvshiryaev
Файл Правка Вид Поиск Терминал Справка
[kvshiryaev@kvshiryaev ~]$ su guest
Пароль:
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test
[guest@kvshiryaev kvshiryaev]$ echo "test2" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test2
[guest@kvshiryaev kvshiryaev]$ echo "test3" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test3
[guest@kvshiryaev kvshiryaev]$ rm .tmp/file01.txt
rm: невозможно удалить './tmp/file01.txt': Отказано в доступе
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod -t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 фев 22 13:33 tmp
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[guest2@kvshiryaev ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt
[guest2@kvshiryaev ~]$
```

Figure 18: Работа с файлом `file01.txt` в директории с `t`

## Снятие атрибута `t`

Повысили свои права до суперпользователя командой `su -`

Выполнили после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`:  
`chmod -t /tmp`.

Покинули режим суперпользователя командой `exit`

От пользователя `guest2` проверили, что атрибута `t` у директории `/tmp` нет: `ls -l / | grep tmp`

```
guest@kvshiryaev:/home/kvshiryaev
Файл Правка Вид Поиск Терминал Справка
[guest@kvshiryaev kvshiryaev]$ echo "test2" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test2
[guest@kvshiryaev kvshiryaev]$ echo "test3" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test3
[guest@kvshiryaev kvshiryaev]$ rm .tmp/file01.txt
rm: невозможно удалить './tmp/file01.txt': Отказано в доступе
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod -t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 фев 22 13:33 tmp
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod +t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$
[guest@kvshiryaev ~]# ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt
```

Figure 19: Снятие атрибута *t*

## Работа с файлом *file01.txt* в директории без *t*

Повторили все действия и, в отличие от предыдущего раза, теперь уже нам удалось удалить файл:



```
guest@kvshiryaev:/home/kvshiryaev
Файл Правка Вид Поиск Терминал Справка
[guest@kvshiryaev kvshiryaev]$ echo "test2" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test2
[guest@kvshiryaev kvshiryaev]$ echo "test3" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test3
[guest@kvshiryaev kvshiryaev]$ rm .tmp/file01.txt
rm: невозможно удалить './tmp/file01.txt': Отказано в доступе
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod -t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 фев 22 13:33 tmp
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod +t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$
[guest@kvshiryaev ~]# ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt
```

Figure 20: Работа с файлом *file01.txt* в директории без *t*

## Возврат атрибута *t*

Повысили свои права с помощью *su*, вернули директории */tmp* атрибут *t*:

```
guest@kvshiryaev:/home/kvshiryaev
Файл Правка Вид Поиск Терминал Справка
[guest@kvshiryaev kvshiryaev]$ echo "test2" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test2
[guest@kvshiryaev kvshiryaev]$ echo "test3" > /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ cat /tmp/file01.txt
test3
[guest@kvshiryaev kvshiryaev]$ rm .tmp/file01.txt
rm: невозможно удалить './tmp/file01.txt': Отказано в доступе
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod -t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 фев 22 13:33 tmp
[guest@kvshiryaev kvshiryaev]$ rm /tmp/file01.txt
[guest@kvshiryaev kvshiryaev]$ su -
Пароль:
[root@kvshiryaev ~]# chmod +t /tmp
[root@kvshiryaev ~]# exit
выход
[guest@kvshiryaev kvshiryaev]$
[guest@kvshiryaev ~]# ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest2 guest2 5 фев 22 13:29 /tmp/file01.txt
```

Figure 21: Возврат атрибута *t*

## Вывод

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.

Получили практические навыки работы в консоли с дополнительными атрибутами.

Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.