

# **Отчёт по лабораторной работе №5**

**Дискреционное разграничение прав в Linux. Исследование влияния  
дополнительных атрибутов**

Волков Фрол НПИбд-01-19

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	6
2.3	Исследование Sticky-бита . . . . .	12
<b>3</b>	<b>Выводы</b>	<b>16</b>
	<b>Список литературы</b>	<b>17</b>

# List of Figures

2.1	подготовка к работе . . . . .	5
2.2	программа simpleid . . . . .	6
2.3	результат программы simpleid . . . . .	7
2.4	программа simpleid2 . . . . .	7
2.5	результат программы simpleid2 . . . . .	9
2.6	программа readfile . . . . .	10
2.7	результат программы readfile . . . . .	11
2.8	результат программы readfile . . . . .	12
2.9	исследование Sticky-бита . . . . .	15

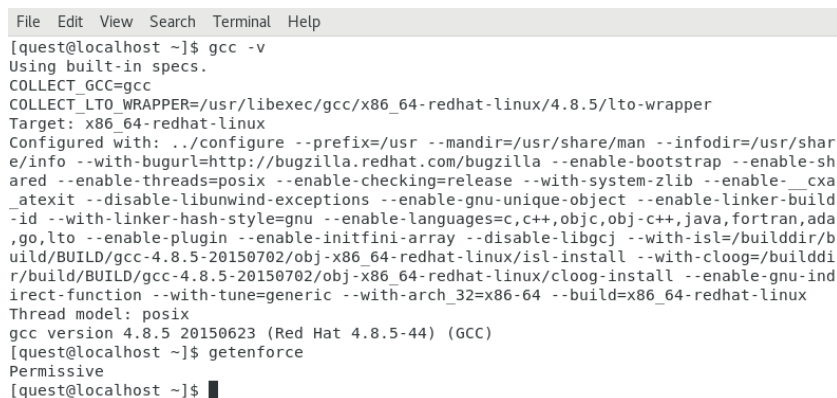
# 1 Цель работы

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

### 2.1 Подготовка

1. Для выполнения части заданий требуются средства разработки приложений. Проверили наличие установленного компилятора gcc командой `gcc -v`: компилятор обнаружен.
2. Чтобы система защиты SELinux не мешала выполнению заданий работы, отключили систему запретов до очередной перезагрузки системы командой `setenforce 0`:
3. Команда `getenforce` вывела `Permissive`:



```
File Edit View Search Terminal Help
[quest@localhost ~]$ gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/4.8.5/lto-wrapper
Target: x86_64-redhat-linux
Configured with: ../configure --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=http://bugzilla.redhat.com/bugzilla --enable-bootstrap --enable-shared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-linker-hash-style=gnu --enable-languages=c,c++,objc,obj-c++,java,fortran,ada,go,lto --enable-plugin --enable-initfini-array --disable-libgck --with-isl=/build/buildd/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/isl-install --with-cloog=/build/buildd/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/cloog-install --enable-gnu-indirect-function --with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Thread model: posix
gcc version 4.8.5 20150623 (Red Hat 4.8.5-44) (GCC)
[quest@localhost ~]$ getenforce
Permissive
[quest@localhost ~]$
```

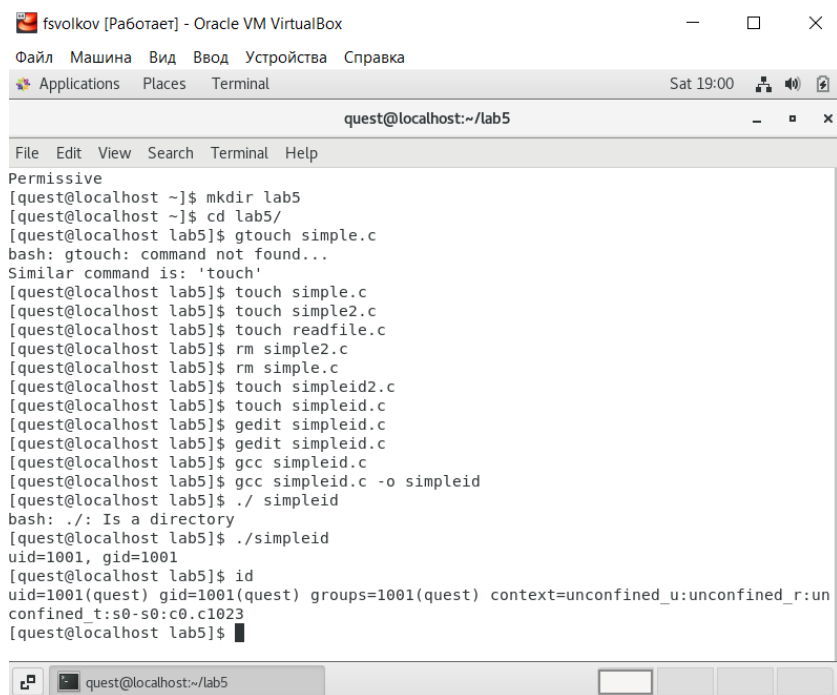
Figure 2.1: подготовка к работе

## 2.2 Изучение механики SetUID

1. Вошли в систему от имени пользователя guest.
2. Написали программу simpleid.c.

Figure 2.2: программа simpleid

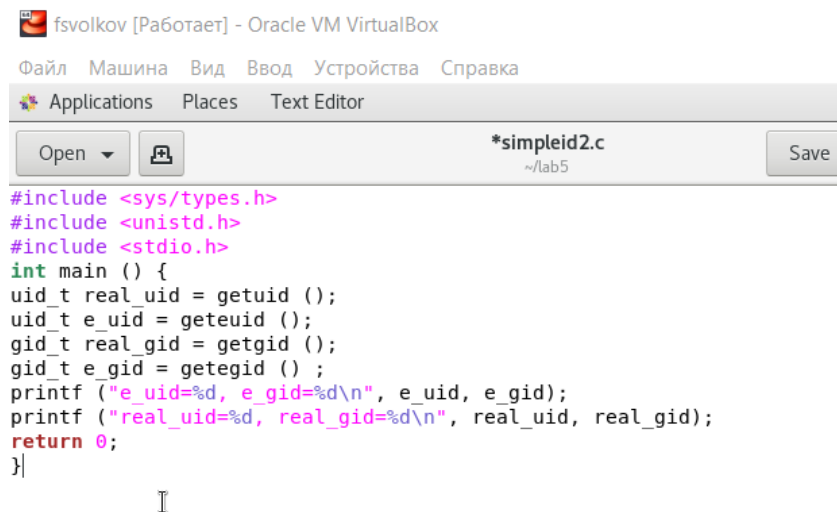
3. Скомпилировали программу и убедились, что файл программы создан: gcc simpleid.c -o simpleid
4. Выполнили программу simpleid командой ./simpleid
5. Выполнили системную программу id с помощью команды id. uid и gid совпадает в обеих программах



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
Sat 19:00
quest@localhost:~/lab5
File  Edit  View  Search  Terminal  Help
Permissive
[quest@localhost ~]$ mkdir lab5
[quest@localhost ~]$ cd lab5/
[quest@localhost lab5]$ gtouch simple.c
bash: gtouch: command not found...
Similar command is: 'touch'
[quest@localhost lab5]$ touch simple.c
[quest@localhost lab5]$ touch simple2.c
[quest@localhost lab5]$ touch readfile.c
[quest@localhost lab5]$ rm simple2.c
[quest@localhost lab5]$ rm simple.c
[quest@localhost lab5]$ touch simpleid2.c
[quest@localhost lab5]$ touch simpleid.c
[quest@localhost lab5]$ gedit simpleid.c
[quest@localhost lab5]$ gcc simpleid.c
[quest@localhost lab5]$ gcc simpleid.c -o simpleid
[quest@localhost lab5]$ ./simpleid
bash: ./: Is a directory
[quest@localhost lab5]$ ./simpleid
uid=1001, gid=1001
[quest@localhost lab5]$ id
uid=1001(quest) gid=1001(quest) groups=1001(quest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[quest@localhost lab5]$
```

Figure 2.3: результат программы simpleid

6. Усложнили программу, добавив вывод действительных идентификаторов.



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Text Editor
Open  *simpleid2.c  Save
~/lab5
#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;
}
```

Figure 2.4: программа simpleid2

7. Скомпилировали и запустили simpleid2.c:

```
gcc simpleid2.c -o simpleid2
./simpleid2
```

8. От имени суперпользователя выполнили команды:

```
chown root:guest /home/guest/simpleid2
chmod u+s /home/guest/simpleid2
```

9. Использовали su для повышения прав до суперпользователя

10. Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

```
ls -l simpleid2
```

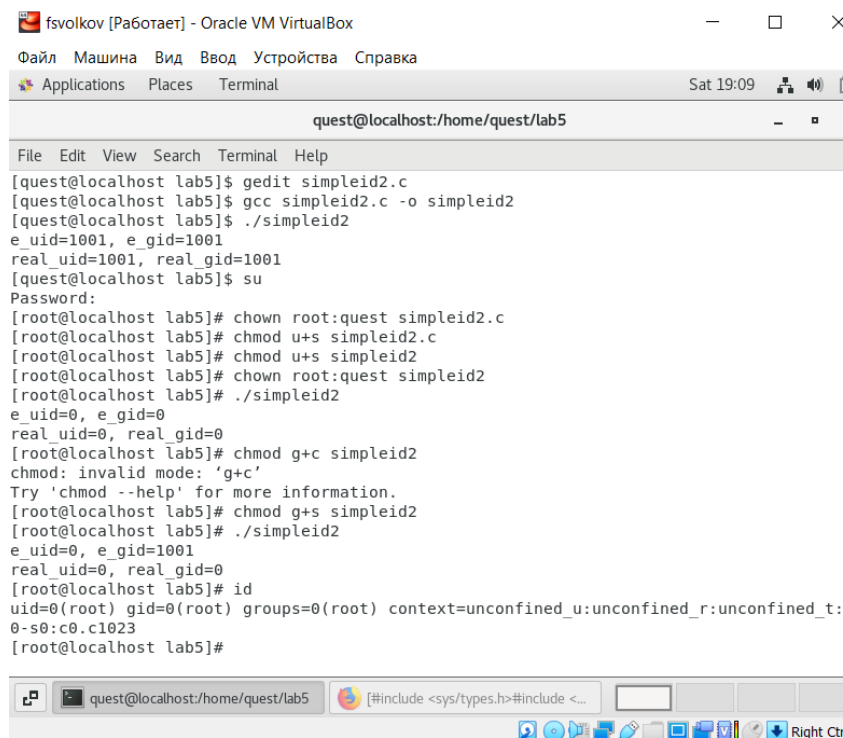
11. Запустили simpleid2 и id:

```
./simpleid2
id
```

Результат выполнения программ теперь немного отличается

12. Проделали тоже самое относительно SetGID-бита.





```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places Terminal Sat 19:09
quest@localhost:/home/quest/lab5
File Edit View Search Terminal Help
[quest@localhost lab5]$ gedit simpleid2.c
[quest@localhost lab5]$ gcc simpleid2.c -o simpleid2
[quest@localhost lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real uid=1001, real gid=1001
[quest@localhost lab5]$ su
Password:
[root@localhost lab5]# chown root:quest simpleid2.c
[root@localhost lab5]# chmod u+s simpleid2.c
[root@localhost lab5]# chmod u+s simpleid2
[root@localhost lab5]# chown root:quest simpleid2
[root@localhost lab5]# ./simpleid2
e_uid=0, e_gid=0
real uid=0, real gid=0
[root@localhost lab5]# chmod g+c simpleid2
chmod: invalid mode: 'g+c'
Try 'chmod --help' for more information.
[root@localhost lab5]# chmod g+s simpleid2
[root@localhost lab5]# ./simpleid2
e_uid=0, e_gid=1001
real uid=0, real gid=0
[root@localhost lab5]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:0-s0:c0.c1023
[root@localhost lab5]#
```

Figure 2.5: результат программы simpleid2

### 13. Написали программу readfile.c

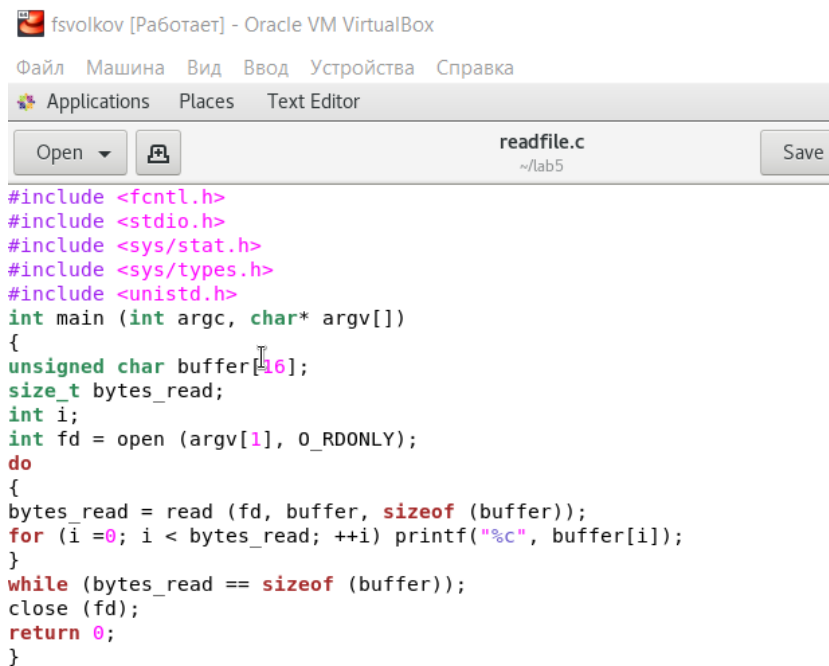


Figure 2.6: программа readfile

14. Откомпилировали её.

```
gcc readfile.c -o readfile
```

15. Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.

```
chown root:guest /home/guest/readfile.c
```

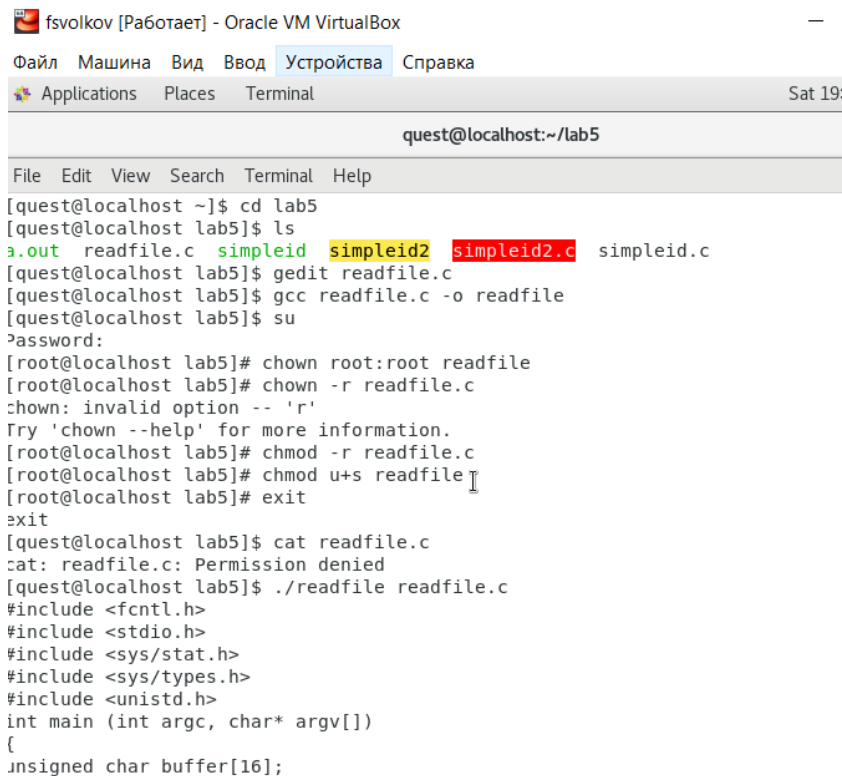
```
chmod 700 /home/guest/readfile.c
```

16. Проверили, что пользователь guest не может прочитать файл readfile.c.

17. Сменили у программы readfile владельца и установили SetU'D-бит.

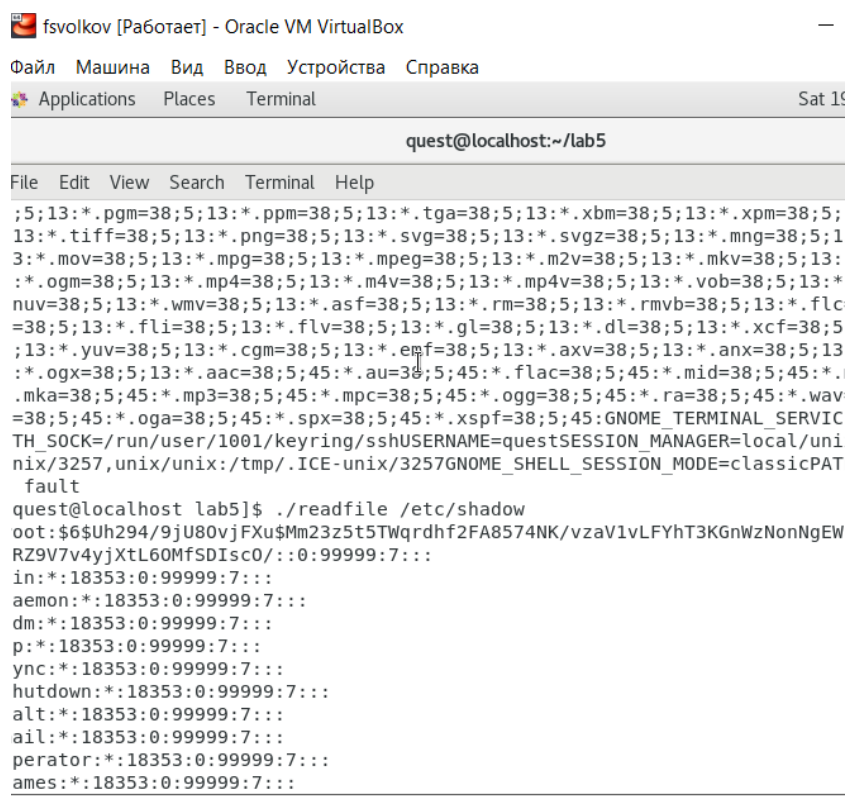
18. Проверили, может ли программа readfile прочитать файл readfile.c

19. Проверили, может ли программа readfile прочитать файл /etc/shadow



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  Sat 19:
quest@localhost:~/lab5
File  Edit  View  Search  Terminal  Help
[quest@localhost ~]$ cd lab5
[quest@localhost lab5]$ ls
a.out  readfile.c  simpleid  simpleid2  simpleid2.c  simpleid.c
[quest@localhost lab5]$ gedit readfile.c
[quest@localhost lab5]$ gcc readfile.c -o readfile
[quest@localhost lab5]$ su
password:
[root@localhost lab5]# chown root:root readfile
[root@localhost lab5]# chown -r readfile.c
chown: invalid option -- 'r'
Try 'chown --help' for more information.
[root@localhost lab5]# chmod -r readfile.c
[root@localhost lab5]# chmod u+s readfile
[root@localhost lab5]# exit
exit
[quest@localhost lab5]$ cat readfile.c
cat: readfile.c: Permission denied
[quest@localhost lab5]$ ./readfile 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];
```

Figure 2.7: результат программы readfile



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  Sat 19
quest@localhost:~/lab5
File  Edit  View  Search  Terminal  Help
;5;13:*.pgm=38;5;13:*.ppm=38;5;13:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;
13:*.tiff=38;5;13:*.png=38;5;13:*.svg=38;5;13:*.svgz=38;5;13:*.mng=38;5;1
3:*.mov=38;5;13:*.mpg=38;5;13:*.mpeg=38;5;13:*.m2v=38;5;13:*.mkv=38;5;13:
:*.ogm=38;5;13:*.mp4=38;5;13:*.m4v=38;5;13:*.mp4v=38;5;13:*.vob=38;5;13:
nuv=38;5;13:*.wmv=38;5;13:*.asf=38;5;13:*.rm=38;5;13:*.rmvb=38;5;13:*.flc
=38;5;13:*.fli=38;5;13:*.flv=38;5;13:*.gl=38;5;13:*.dl=38;5;13:*.xcf=38;5
;13:*.yuv=38;5;13:*.cgm=38;5;13:*.emf=38;5;13:*.axv=38;5;13:*.anx=38;5;13
:*.ogx=38;5;13:*.aac=38;5;45:*.au=38;5;45:*.flac=38;5;45:*.mid=38;5;45:*.
.mka=38;5;45:*.mp3=38;5;45:*.mpc=38;5;45:*.ogg=38;5;45:*.ra=38;5;45:*.wav
=38;5;45:*.oga=38;5;45:*.spx=38;5;45:*.xspf=38;5;45:GNOME_TERMINAL_SERVIC
TH_SOCKET=/run/user/1001/keyring/sshUSERNAME=questSESSION_MANAGER=local/uni
nix/3257,unix/unix:/tmp/.ICE-unix/3257GNOME_SHELL_SESSION_MODE=classicPAT
fault
quest@localhost lab5]$ ./readfile /etc/shadow
oot:$6$Uh294/9jU80vjFXu$Mm23z5t5TWqrdf2FA8574NK/vzaV1vLFYhT3KGnWzNonNgEW
RZ9V7v4yJXtL60MfSDisc0/::0:99999:7:::
in*:18353:0:99999:7:::
aemon*:18353:0:99999:7:::
dm*:18353:0:99999:7:::
p*:18353:0:99999:7:::
ync*:18353:0:99999:7:::
hutdown*:18353:0:99999:7:::
alt*:18353:0:99999:7:::
ail*:18353:0:99999:7:::
perator*:18353:0:99999:7:::
ames*:18353:0:99999:7:::
```

Figure 2.8: результат программы readfile

## 2.3 Исследование Sticky-бита

1. Выяснили, установлен ли атрибут Sticky на директории /tmp:

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

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

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

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

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

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

Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме «остальных пользователей».

4. От пользователя (не являющегося владельцем) попробовали прочитать файл /file01.txt:

```
cat /file01.txt
```

5. От пользователя попробовали дозаписать в файл /file01.txt слово test3 командой:

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

6. Проверили содержимое файла командой:

```
cat /file01.txt
```

В файле теперь записано:

```
Test  
Test2
```

7. От пользователя попробовали записать в файл /tmp/file01.txt слово test4, стерев при этом всю имеющуюся в файле информацию командой. Для этого воспользовалась командой `echo "test3" > /tmp/file01.txt`

8. Проверили содержимое файла командой

```
cat /tmp/file01.txt
```

9. От пользователя попробовали удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt`, однако получила отказ.

10. От суперпользователя командой выполнили команду, снимающую атрибут t (Sticky-бит) с директории /tmp:

```
chmod -t /tmp
```

Покинули режим суперпользователя командой exit.

11. От пользователя проверили, что атрибута t у директории /tmp нет:

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

12. Повторили предыдущие шаги. Получилось удалить файл

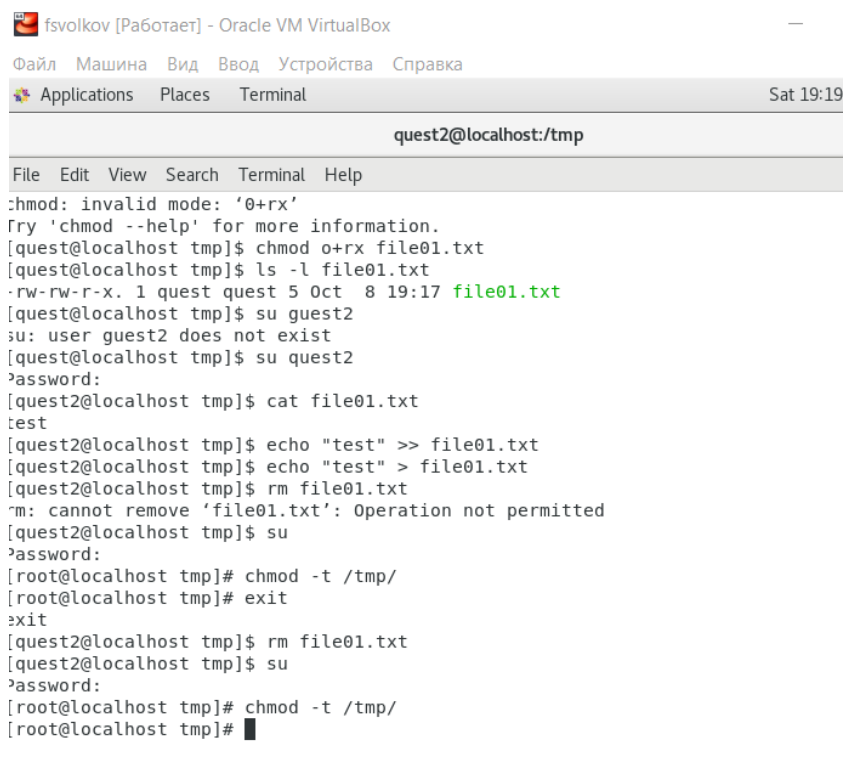
13. Удалось удалить файл от имени пользователя, не являющегося его владельцем.

14. Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp :

```
su
```

```
chmod +t /tmp
```

```
exit
```



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  Sat 19:19
quest2@localhost:/tmp
File Edit View Search Terminal Help
chmod: invalid mode: '0+rx'
Try 'chmod --help' for more information.
[quest@localhost tmp]$ chmod o+rx file01.txt
[quest@localhost tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 quest quest 5 Oct  8 19:17 file01.txt
[quest@localhost tmp]$ su guest2
su: user guest2 does not exist
[quest@localhost tmp]$ su quest2
password:
[quest2@localhost tmp]$ cat file01.txt
test
[quest2@localhost tmp]$ echo "test" >> file01.txt
[quest2@localhost tmp]$ echo "test" > file01.txt
[quest2@localhost tmp]$ rm file01.txt
rm: cannot remove 'file01.txt': Operation not permitted
[quest2@localhost tmp]$ su
password:
[root@localhost tmp]# chmod -t /tmp/
[root@localhost tmp]# exit
exit
[quest2@localhost tmp]$ rm file01.txt
[quest2@localhost tmp]$ su
password:
[root@localhost tmp]# chmod -t /tmp/
[root@localhost tmp]#
```

Figure 2.9: исследование Sticky-бита

## 3 Выводы

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.



# Список литературы

1. КОМАНДА CHATTR В LINUX
2. chattr