

# Лабораторная работа №5

---

Fogileva Ksenia Mikhailovna<sup>1</sup>

29.10.2021, Moscow, Russian Federation

<sup>1</sup>RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной  
работы

---

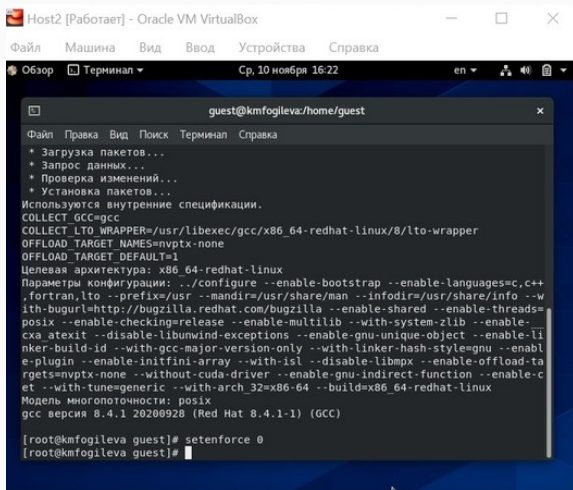
## Цель выполнения лабораторной работы

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 выполнения лабораторной работы

---

# 1. Загрузила gcc и отключите систему запретов до очередной перезагрузки системы. (рис.1)

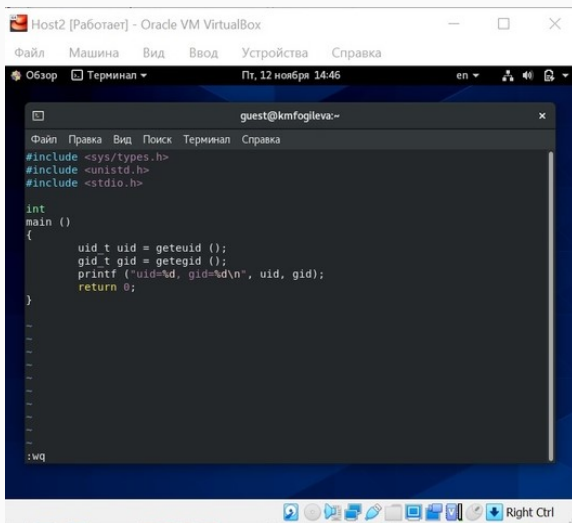


```
guest@kmfogleva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
* Загрузка пакетов...
* Запрос данных...
* Проверка изменений...
* Установка пакетов...
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/8/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ./configure --enable-bootstrap --enable-languages=c,c++
,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --w
ith-bugurl=http://bugzilla.redhat.com/bugzilla --enable-shared --enable-threads=
posix --enable-checking=release --enable-multilib --with-system-zlib --enable-
cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-li
nker-build-id --with-gcc-major-version-only --with-linker-hash-style=gnu --enabl
e-plugin --enable-initfini-array --with-isl --disable-libmpx --enable-offload-ta
rgets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-c
et --with-tune=generic --with-arch_32=x86_64 --build=x86_64-redhat-linux
Модель многопоточности: posix
gcc версия 8.4.1 20200928 (Red Hat 8.4.1-1) (GCC)

[root@kmfogleva guest]# setenforce 0
[root@kmfogleva guest]#
```

Figure 1: Рис. 1.

## 2. Создала программу simpleid.c (рис.2).



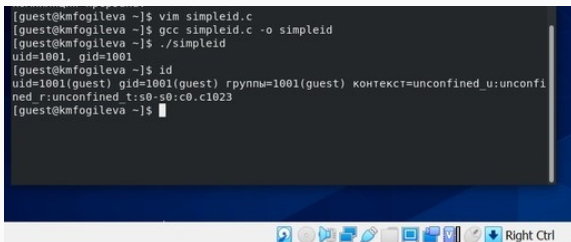
The screenshot shows a terminal window titled "Host2 [Работает] - Oracle VM VirtualBox". The terminal is running a program named "simpleid.c". The code is as follows:

```
guest@kmfogileva:~  
Файл Правка Вид Поиск Терминал Справка  
Обзор Терминал Пт, 12 ноября 14:46 en  
#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;  
}
```

The terminal window also shows a status bar at the bottom with various icons and the text "Right Ctrl".

Figure 2: Рис. 2.

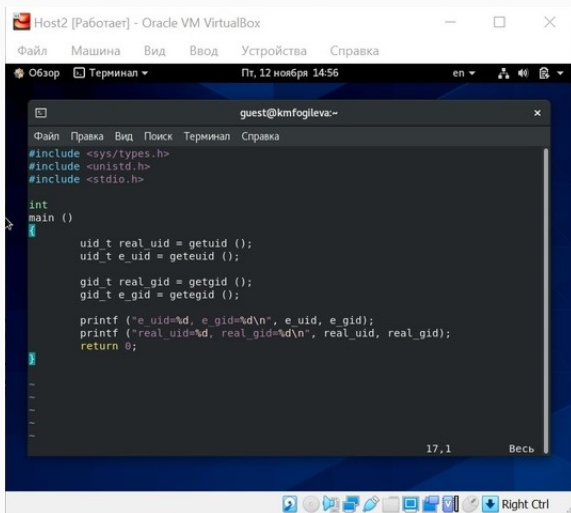
3. Скомпилировала и выполнила программу simpleid, затем запустила id. Результаты совпали. (рис.3).

A terminal window with a dark background and white text. The window shows a series of commands and their outputs. The commands are: 'vim simpleid.c', 'gcc simpleid.c -o simpleid', './simpleid', and 'id'. The outputs are: 'uid=1001, gid=1001' and 'uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023'. The terminal window is titled 'Terminal' and has a standard Linux desktop environment at the bottom with various icons and a 'Right Ctrl' button.

```
[guest@kmfogleva ~]$ vim simpleid.c
[guest@kmfogleva ~]$ gcc simpleid.c -o simpleid
[guest@kmfogleva ~]$ ./simpleid
uid=1001, gid=1001
[guest@kmfogleva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@kmfogleva ~]$
```

Figure 3: Рис. 3.

#### 4. Создала программу simpleid2.ca (рис.4).



Host2 [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал Пт, 12 ноября 14:56 en

guest@kmfogileva:~

Файл Правка Вид Поиск Терминал Справка

```
#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;
}
```

17,1 Весь

Right Ctrl

Figure 4: Рис. 4.



## 5. . Скомпилировала и запустила simpleid2.c (рис.5).

```
real_gid
[guest@kmfogleva ~]$ vim simpleid2.c
[guest@kmfogleva ~]$ gcc simpleid2.c -o simpleid
[guest@kmfogleva ~]$ ./simpleid2
bash: ./simpleid2: Нет такого файла или каталога
[guest@kmfogleva ~]$ gcc simpleid2.c -o simpleid2
[guest@kmfogleva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chown root:guest /home/guest/simpleid2
[root@kmfogleva guest]# chmod u+s /home/guest/simpleid2
[root@kmfogleva guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 ноя 12 14:57 simpleid2
[root@kmfogleva guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@kmfogleva guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
[root@kmfogleva guest]#
```

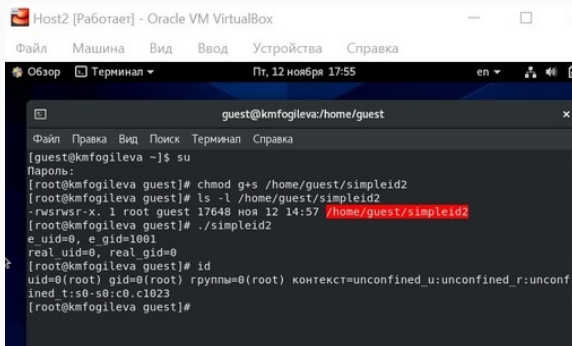
Figure 5: Рис. 5.

6. Повысила права, выполнила команды, выполнила проверку правильности выполнения команд, запустила simpleid2 и id (рис.6).

```
real_gid
[guest@kmfogleva ~]$ vim simpleid2.c
[guest@kmfogleva ~]$ gcc simpleid2.c -o simpleid
[guest@kmfogleva ~]$ ./simpleid2
bash: ./simpleid2: Нет такого файла или каталога
[guest@kmfogleva ~]$ gcc simpleid2.c -o simpleid2
[guest@kmfogleva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chown root:guest /home/guest/simpleid2
[root@kmfogleva guest]# chmod u+s /home/guest/simpleid2
[root@kmfogleva guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 ноя 12 14:57 simpleid2
[root@kmfogleva guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@kmfogleva guest]# id
uid=0(root) gid=0(root) rpyнны=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@kmfogleva guest]#
```

Figure 6: Рис. 6.

## 7. Прodelайте тоже самое относительно SetGID-бита (рис.7).

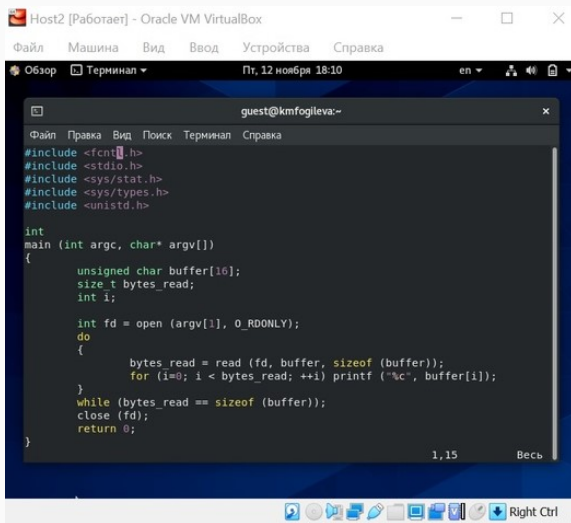


The screenshot shows a terminal window titled "Host2 [Работает] - Oracle VM VirtualBox". The terminal is running a guest OS named "kmfogleva". The user "guest" is at the prompt "guest@kmfogleva:/home/guest". The user enters "su" to become root. The root prompt is "[root@kmfogleva guest]". The user enters "chmod g+s /home/guest/simpleid2". The user enters "ls -l /home/guest/simpleid2", which shows the file permissions as "-rwsrwsr-x. 1 root guest 17648 ноя 12 14:57 /home/guest/simpleid2". The user enters "./simpleid2", which outputs "e\_uid=0, e\_gid=1001" and "real\_uid=0, real\_gid=0". The user enters "id", which outputs "uid=0(root) gid=0(root) группы=0(root) контекст=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023". The user enters "#".

```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Пт, 12 ноября 17:55  en  [иконки]
guest@kmfogleva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chmod g+s /home/guest/simpleid2
[root@kmfogleva guest]# ls -l /home/guest/simpleid2
-rwsrwsr-x. 1 root guest 17648 ноя 12 14:57 /home/guest/simpleid2
[root@kmfogleva guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@kmfogleva guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@kmfogleva guest]#
```

Figure 7: Рис. 7.

## 8. Создала программу readfile.c (рис.8).



The image shows a screenshot of a VirtualBox window titled "Host2 [Работает] - Oracle VM VirtualBox". Inside the window is a terminal window titled "guest@kmfogleva:~". The terminal displays the code for a C program named "readfile.c". The code includes headers for `fcntl.h`, `stdio.h`, `sys/stat.h`, `sys/types.h`, and `unistd.h`. The `main` function takes `argc` and `argv` as arguments. It declares a `buffer` of size 16, a `bytes_read` variable, and an `i` index. It opens the file specified in `argv[1]` in read-only mode. It then enters a loop where it reads data from the file into the buffer and prints each character. The loop continues until the end of the file is reached. Finally, it closes the file and returns 0.

```
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

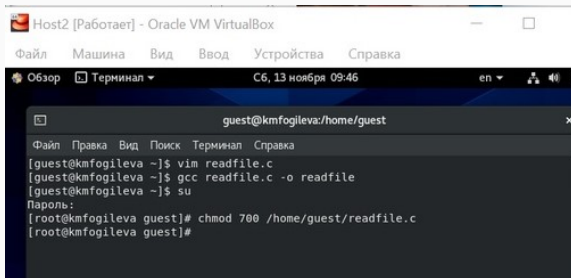
int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    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;
}
```

1,15    Весь

Figure 8: Рис. 8.

## 9. Смените владельца у файла readfile.c (рис.9).



The screenshot shows a VirtualBox window titled "Host2 [Работаег] - Oracle VM VirtualBox". Inside, a terminal window is open with the title "guest@kmfogleva:/home/guest". The terminal shows the following commands and output:

```
guest@kmfogleva ~]$ vim readfile.c
guest@kmfogleva ~]$ gcc readfile.c -o readfile
guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chmod 700 /home/guest/readfile.c
[root@kmfogleva guest]#
```

Figure 9: Рис. 9.

10. Проверила, что пользователь `guest` не может прочитать файл `readfile.c`.  
(рис.10)

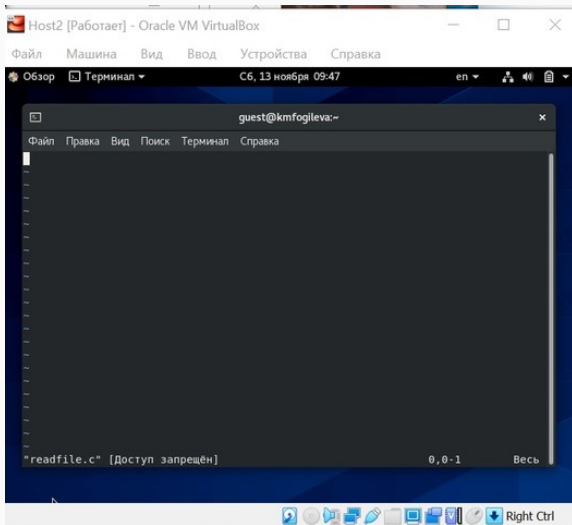
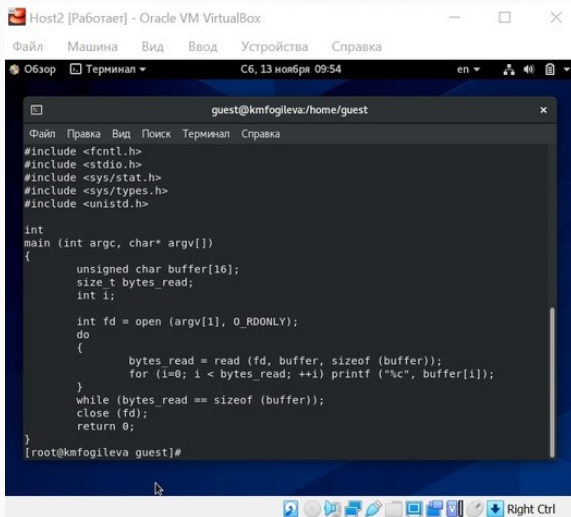


Figure 10: Рис. 10.

11. Сменила у программы readfile владельца и установила SetU'D-бит. Проверила, может ли программа readfile прочитать файл readfile.c (рис.11).



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  C6, 13 ноября 09:54  en  [иконки]
guest@kmfogleva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
#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;
}
[root@kmfogleva guest]#
```

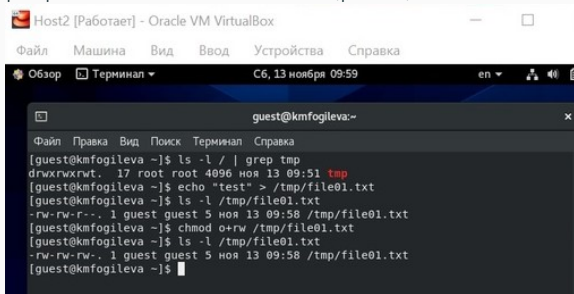
Figure 11: Рис. 11.





13. Выяснила, установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создала файл file01.txt в директории /tmp

со словом test. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись (рис.13)

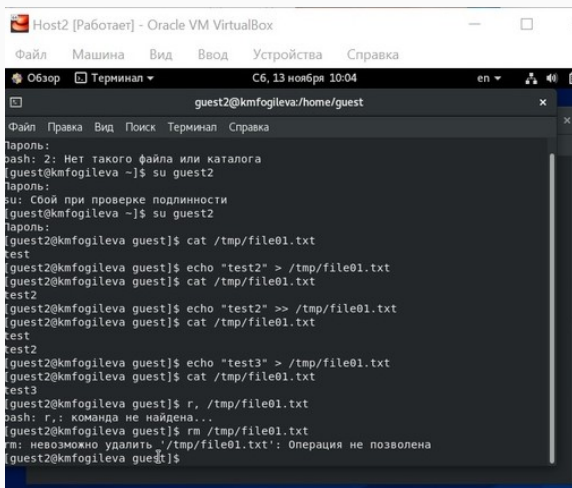


```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  C6, 13 ноября 09:59  en  [иконки]

guest@kmfogleva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@kmfogleva ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 ноя 13 09:51 tmp
[guest@kmfogleva ~]$ echo "test" > /tmp/file01.txt
[guest@kmfogleva ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 13 09:58 /tmp/file01.txt
[guest@kmfogleva ~]$ chmod o+rw /tmp/file01.txt
[guest@kmfogleva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ноя 13 09:58 /tmp/file01.txt
[guest@kmfogleva ~]$
```

14. Выполнила действия от имени пользователя guest2. Не получилось только удалить файл. (рис.14)



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  C6, 13 ноября 10:04  en  [иконки]

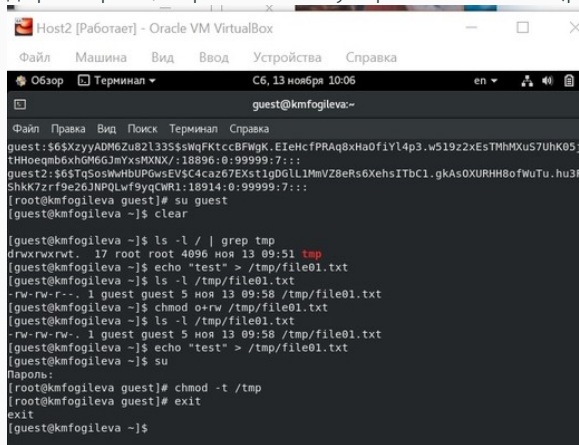
guest2@kmfogleva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка

Пароль:
bash: 2: Нет такого файла или каталога
[guest@kmfogleva ~]$ su guest2
Пароль:
su: Сбой при проверке подлинности
[guest@kmfogleva ~]$ su guest2
Пароль:
[guest2@kmfogleva guest]$ cat /tmp/file01.txt
test
[guest2@kmfogleva guest]$ echo "test2" > /tmp/file01.txt
[guest2@kmfogleva guest]$ cat /tmp/file01.txt
test2
[guest2@kmfogleva guest]$ echo "test2" >> /tmp/file01.txt
[guest2@kmfogleva guest]$ cat /tmp/file01.txt
test
test2
[guest2@kmfogleva guest]$ echo "test3" > /tmp/file01.txt
[guest2@kmfogleva guest]$ cat /tmp/file01.txt
test3
[guest2@kmfogleva guest]$ r, /tmp/file01.txt
bash: r,: команда не найдена...
[guest2@kmfogleva guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@kmfogleva guest]$
```

Figure 13: Рис. 14.

## 15. Выполнила команду, снимающую атрибут t (Sticky-бит) с

директории /tmp от имени суперпользователя. (рис.15).



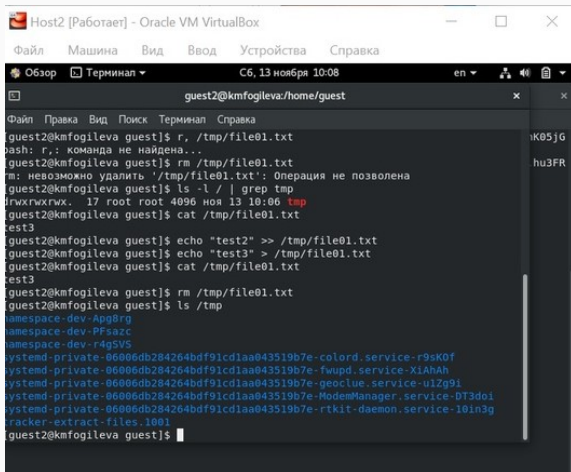
```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  C6, 13 ноября 10:06  en  [иконки]

guest@kmfogleva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
guest:$6$XzyyADM6Zu82l33S$WqFKtccBFwGK.EIeHcfPRAq8xHa0fiYl4p3.w519z2xEsTMhMXuS7UhK05;
tHHoeqmb6xhGM6GJmYxsMXNX/:18896:0:99999:7:::
guest2:$6$TqSosWwHbUPGwsEV$C4caz67EXstlgDGLL1MmVZBeRs6XehsITbC1.gkAsOXURHh8ofWuTu.hu3F
ShkK7zrf9e26JNPQLwf9yqCWR1:18914:0:99999:7:::
[root@kmfogleva guest]# su guest
[guest@kmfogleva ~]$ clear

[guest@kmfogleva ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 ноя 13 09:51 tmp
[guest@kmfogleva ~]$ echo "test" > /tmp/file01.txt
[guest@kmfogleva ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 13 09:58 /tmp/file01.txt
[guest@kmfogleva ~]$ chmod o+rw /tmp/file01.txt
[guest@kmfogleva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ноя 13 09:58 /tmp/file01.txt
[guest@kmfogleva ~]$ echo "test" > /tmp/file01.txt
[guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chmod -t /tmp
[root@kmfogleva guest]# exit
exit
[guest@kmfogleva ~]$
```

16. Повторите предыдущие шаги от имени пользователя guest2, теперь можно удалить файл. (рис.16)



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

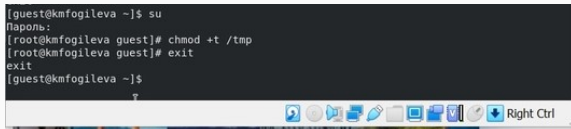
Обзор  Терминал  C6, 13 ноября 10:08  en  [иконки]

guest2@kmfogleva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка

guest2@kmfogleva guest]$ r, /tmp/file01.txt
bash: r,: команда не найдена...
guest2@kmfogleva guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': операция не позволена
guest2@kmfogleva guest]$ ls -l / | grep tmp
lrwxrwxrwx.  17 root root 4096 ноя 13 10:06 tmp
guest2@kmfogleva guest]$ cat /tmp/file01.txt
test3
guest2@kmfogleva guest]$ echo "test2" >> /tmp/file01.txt
guest2@kmfogleva guest]$ echo "test3" > /tmp/file01.txt
guest2@kmfogleva guest]$ cat /tmp/file01.txt
test3
guest2@kmfogleva guest]$ rm /tmp/file01.txt
guest2@kmfogleva guest]$ ls /tmp
namespace-dev-Apg8rq
namespace-dev-PFsazc
namespace-dev-r4gSVS
systemd-private-06006db284264bdf91cd1aa043519b7e-color.service-r9sK0f
systemd-private-06006db284264bdf91cd1aa043519b7e-fwupd.service-XiAhAh
systemd-private-06006db284264bdf91cd1aa043519b7e-geoclue.service-ulZg9i
systemd-private-06006db284264bdf91cd1aa043519b7e-ModemManager.service-DT3d0i
systemd-private-06006db284264bdf91cd1aa043519b7e-rtkit-daemon.service-10in3g
cracker-extract-files.1001
guest2@kmfogleva guest]$
```

Figure 14: Рис. 16.

## 17. Повысила свои права до суперпользователя и вернула атрибут `t` на директорию `/tmp`. (рис. 17)

A terminal window with a dark background. The text shows a user switching from 'guest' to 'root' using 'su', then running 'chmod +t /tmp' as root, and finally exiting back to the 'guest' user. The desktop environment at the bottom includes a taskbar with various icons and a 'Right Ctrl' button.

```
[guest@kmfogleva ~]$ su
Пароль:
[root@kmfogleva guest]# chmod +t /tmp
[root@kmfogleva guest]# exit
exit
[guest@kmfogleva ~]$
```

Figure 15: Рис. 17.

## Выводы

---

Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессы пользователей, а также влияние бита Sticky на запись и удаление файлов.

Спасибо за внимание!