

Отчёт по лабораторной работе №5

дисциплина: Информационная безопасность

Фогилева ксения Михайловна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	17

List of Tables

List of Figures

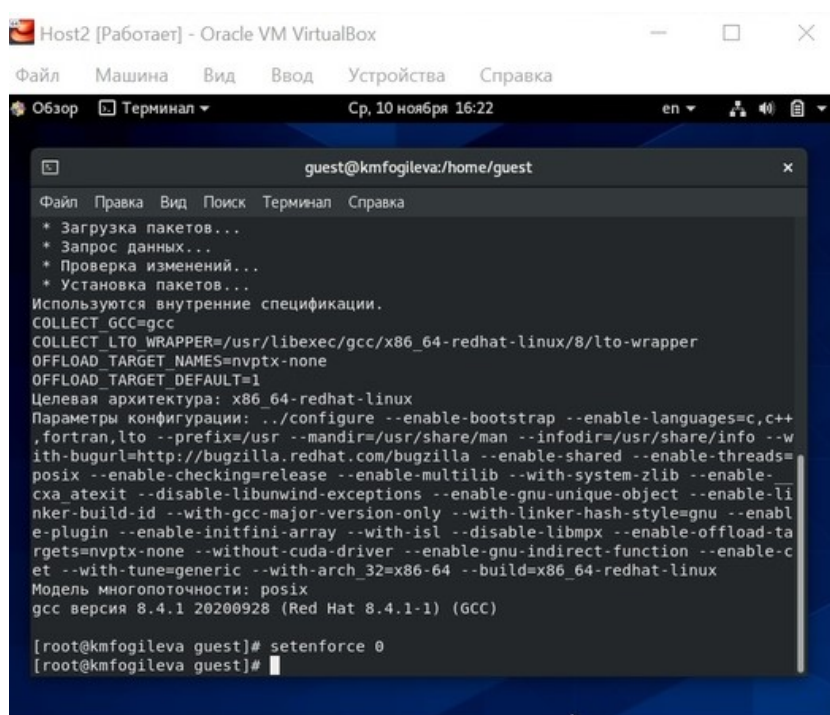
2.1	Рис. 1.	6
2.2	Рис. 2.	7
2.3	Рис. 3.	7
2.4	Рис. 4.	8
2.5	Рис. 5.	8
2.6	Рис. 6.	9
2.7	Рис. 7.	9
2.8	Рис. 8.	10
2.9	Рис. 9.	10
2.10	Рис. 10.	11
2.11	Рис. 11.	12
2.12	Рис. 12.	13
2.13	Рис. 13.	14
2.14	Рис. 14.	14
2.15	Рис. 15.	15
2.16	Рис. 16.	15
2.17	Рис. 17.	16

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

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



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Ср, 10 ноября 16:22  en  [иконки]
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-
ска_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 2.1: Рис. 1.

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

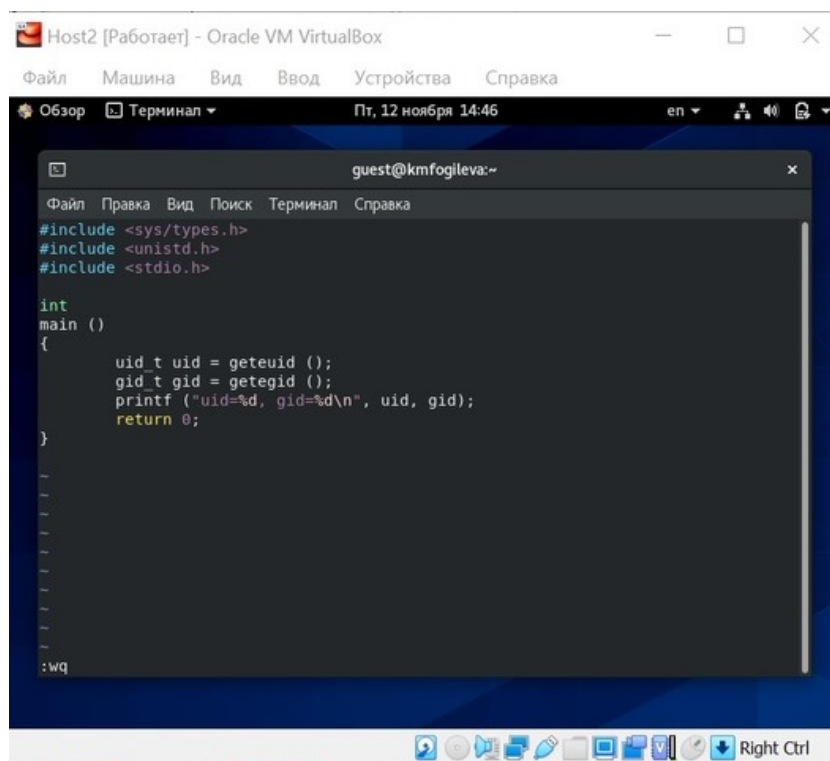


Figure 2.2: Рис. 2.

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

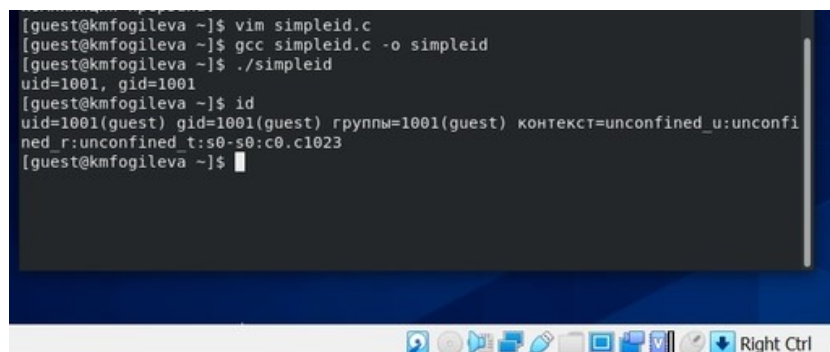


Figure 2.3: Рис. 3.

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

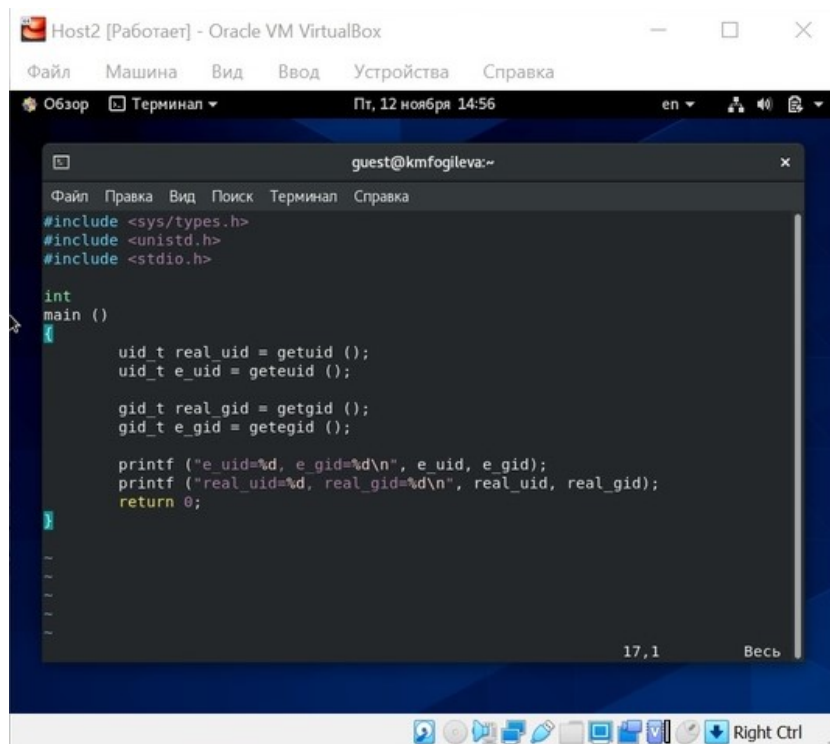


Figure 2.4: Рис. 4.

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

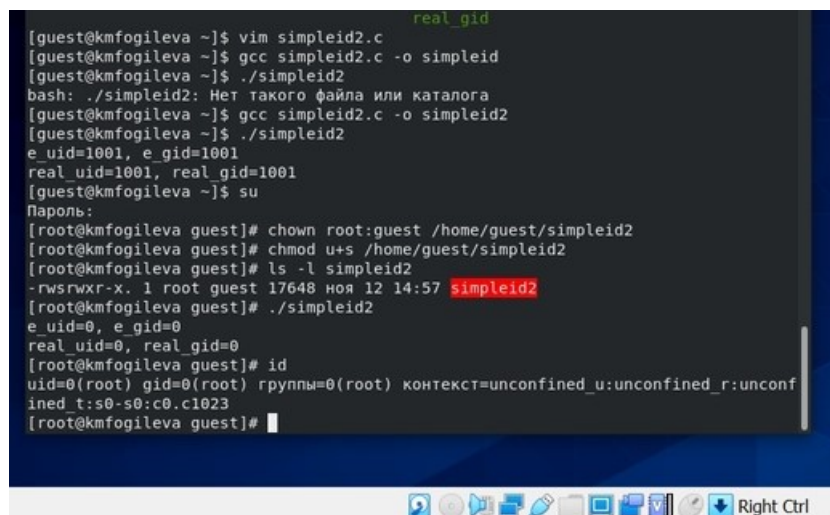


Figure 2.5: Рис. 5.

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) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@kmfogleva guest]#
```

Figure 2.6: Рис. 6.

7. Проделайте тоже самое относительно SetGID-бита (рис.7).

```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Пт, 12 ноября 17:55  en
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 2.7: Рис. 7.

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

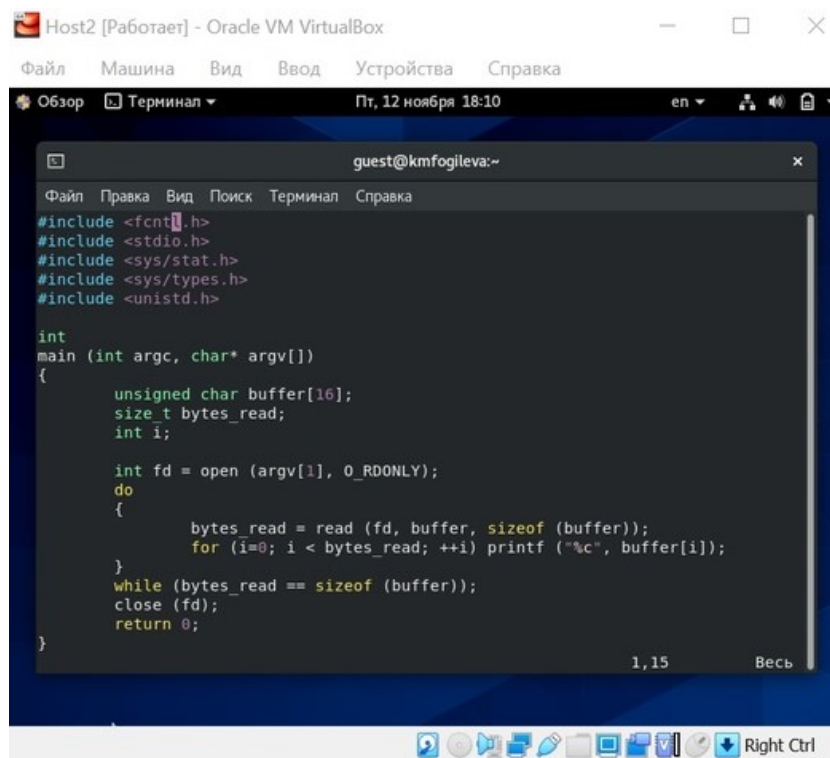


Figure 2.8: Рис. 8.

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

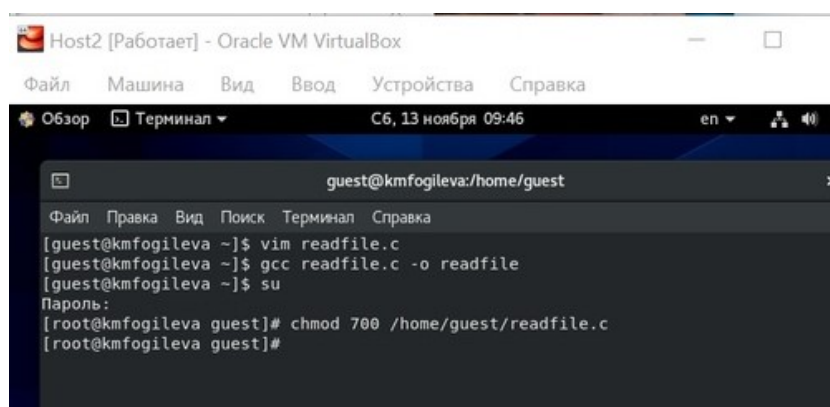


Figure 2.9: Рис. 9.

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

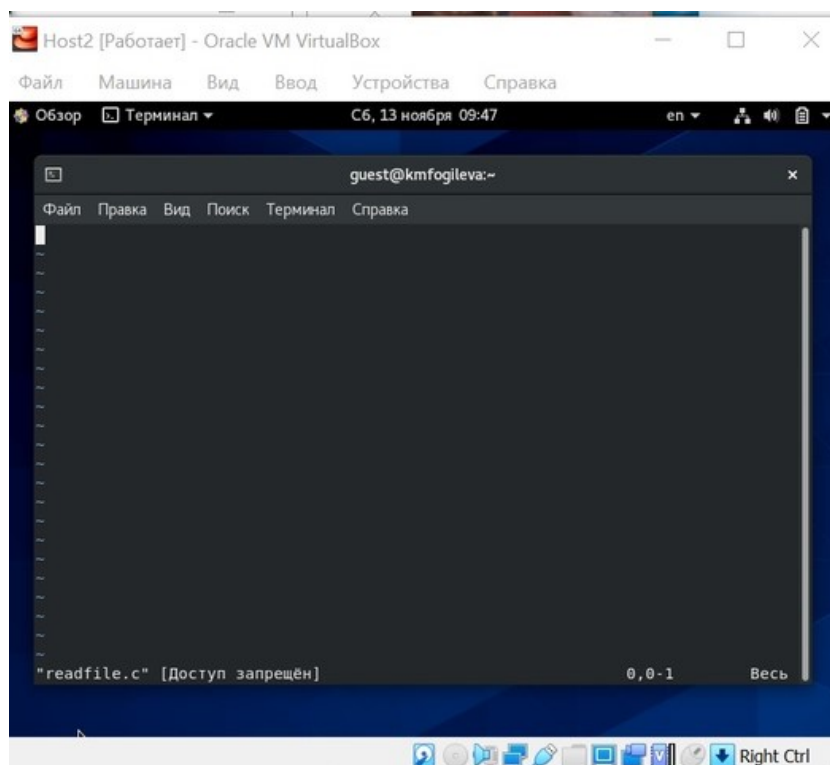


Figure 2.10: Рис. 10.

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

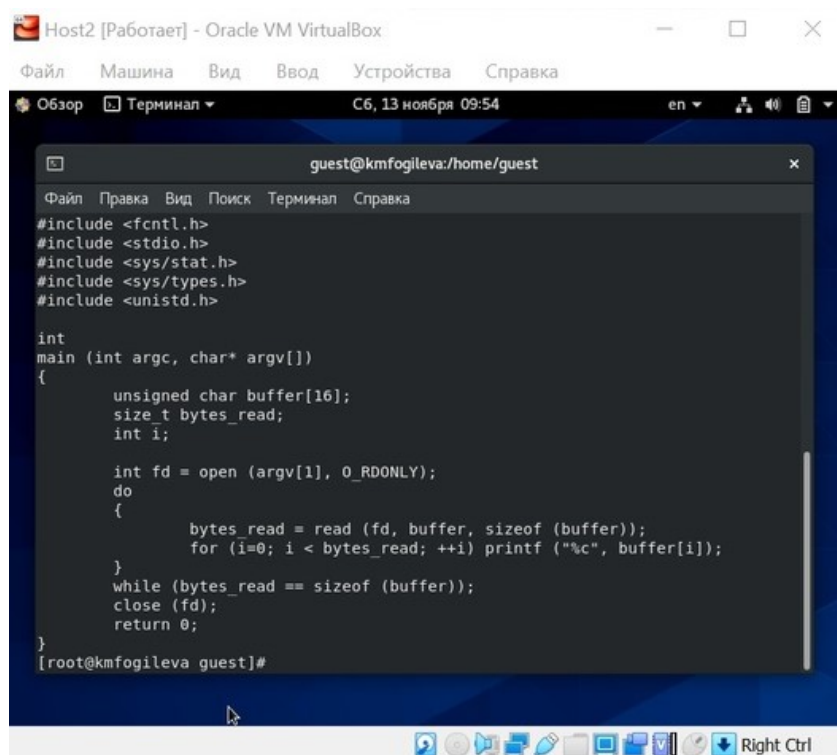


Figure 2.11: Рис. 11.

12. Проверила, может ли программа readfile прочитать файл /etc/shadow (рис.12)

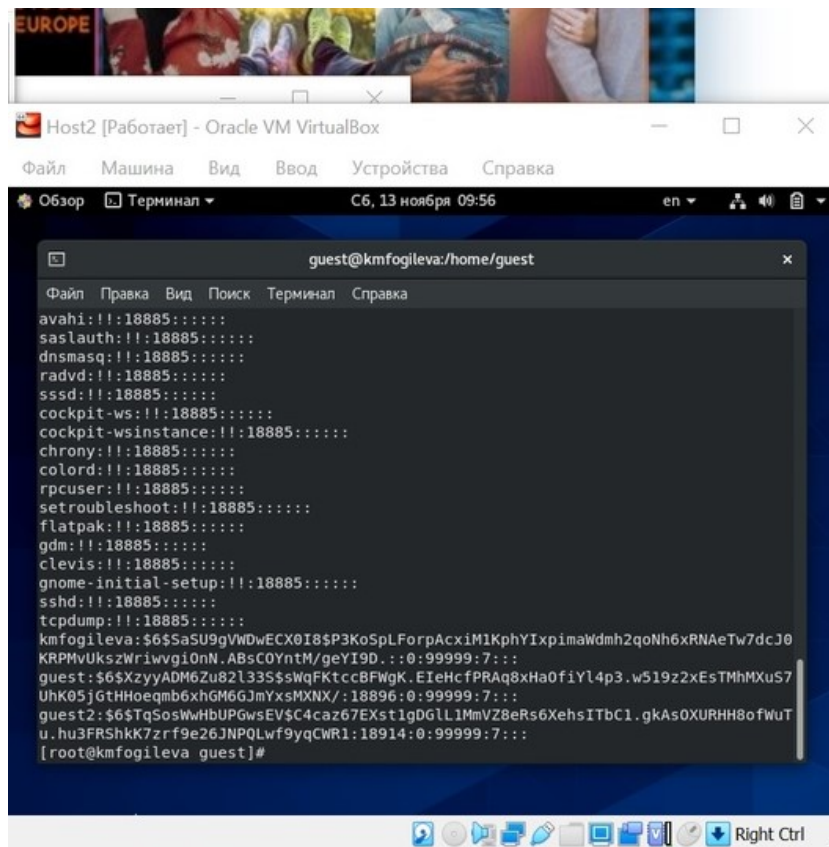


Figure 2.12: Рис. 12.

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)

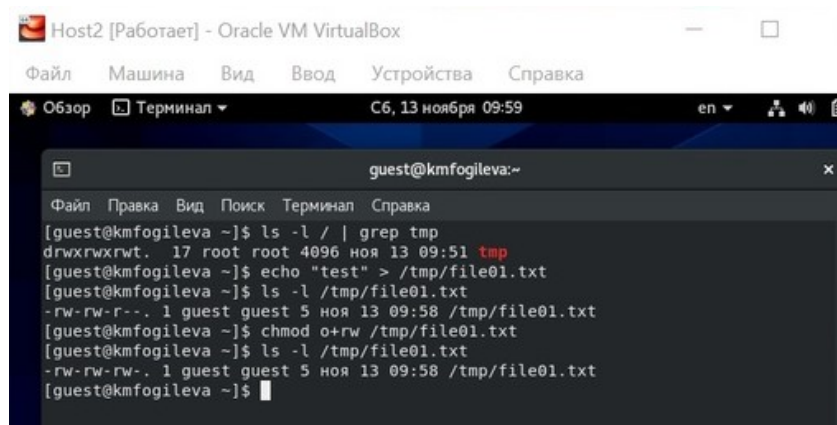


Figure 2.13: Рис. 13.

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

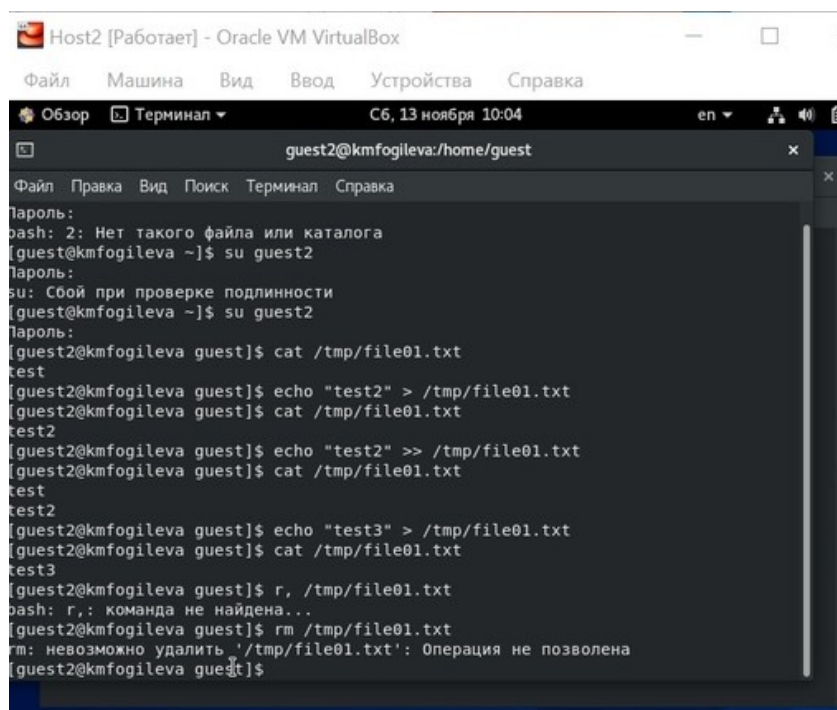
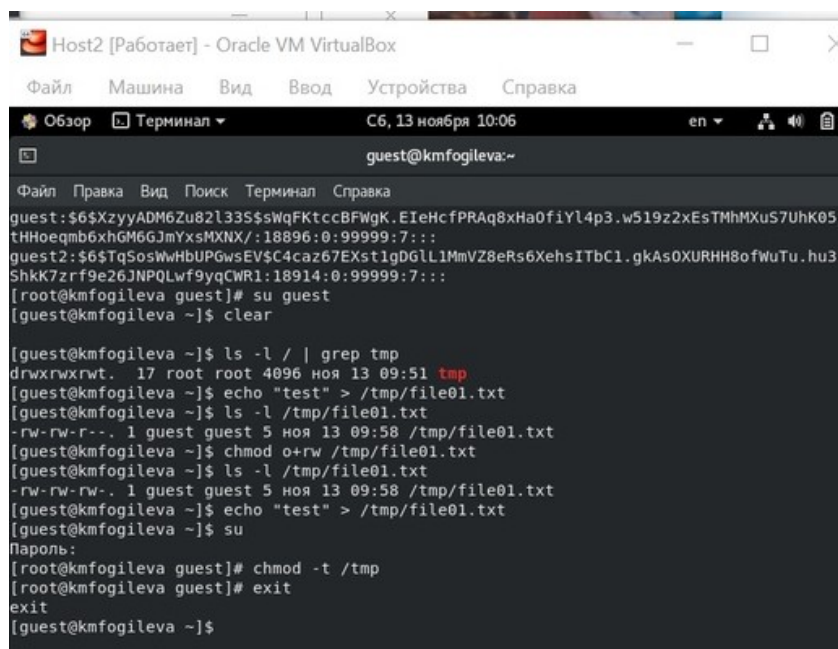


Figure 2.14: Рис. 14.

15. Выполнила команду, снимающую атрибут t (Sticky-бит) с директории /tmp от имени суперпользователя. (рис.15).

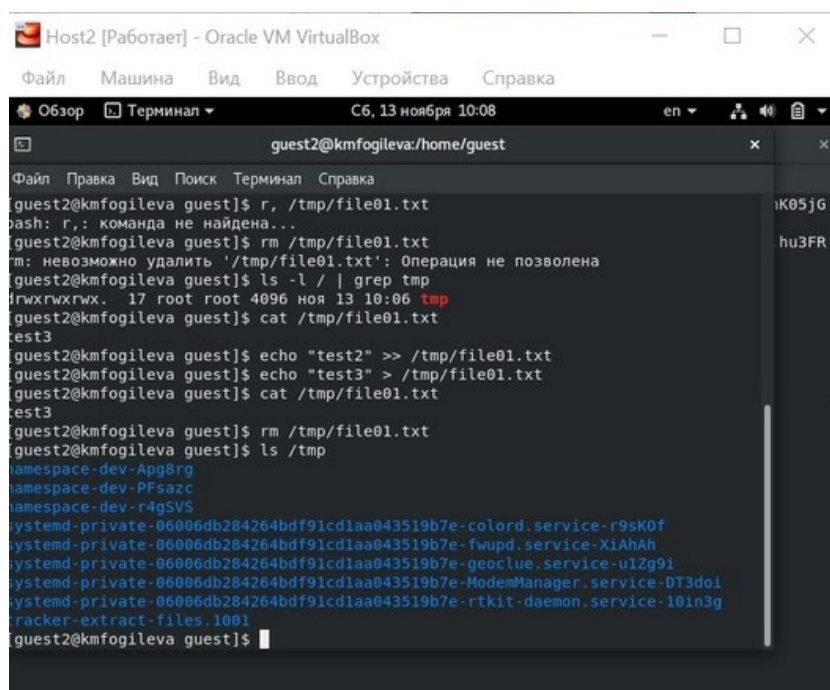


```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  C6, 13 ноября 10:06  en
guest@kmfogleva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
guest:$6$XzyyADM6Zu82l335$S$WqFKtccBFWgK.EIeHcfPRAq8xHa0fiYl4p3.w519z2xEsTMhMXuS7UhK05;
tHHoeqmb6xhG6GJmYxsMXNX/:18896:0:99999:7:::
guest2:$6$TqSosWwHbUPGwsEV$C4caz67EXst1gD6lL1MmVZ8eRs6XehsITbC1.gkAs0XURHH8ofWuTu.hu3F
ShkK7zrf9e26JNPQLwf9yqCWR1:18914:0:99999:7:::
[root@kmfogleva guest]# su guest
[guest@kmfogleva ~]$ 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 ~]$
```

Figure 2.15: Рис. 15.

- 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
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
drwxrwxrwx. 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-Apg8rg
namespace-dev-PFsazc
namespace-dev-r4g5VS
systemd-private-06006db284264bdf91cd1aa043519b7e-color.service-r9sK0f
systemd-private-06006db284264bdf91cd1aa043519b7e-fwupd.service-XiAhAh
systemd-private-06006db284264bdf91cd1aa043519b7e-geoclue.service-u1Zg9i
systemd-private-06006db284264bdf91cd1aa043519b7e-ModemManager.service-DT3doi
systemd-private-06006db284264bdf91cd1aa043519b7e-rtkit-daemon.service-10in3g
cracker-extract-files.1001
[guest2@kmfogleva guest]$
```

Figure 2.16: Рис. 16.

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

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

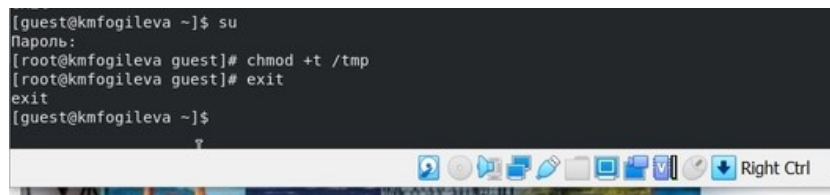


Figure 2.17: Рис. 17.

3 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.