

Лабораторная работа №5

Информационная безопасность

Леонтьева Ксения Андреевна | НПМбд-01-19

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
3.1	Создание программы	6
3.2	Исследование Sticky-бита	14
4	Выводы	18
	Список литературы	19

Список иллюстраций

3.1	Предварительная подготовка	6
3.2	Команда “whereis”	7
3.3	Вход в систему и создание программы	7
3.4	Код программы simpleid.c	8
3.5	Компиляция и выполнение программы simpleid	8
3.6	Усложнение программы	9
3.7	Переименование программы в simpleid2.c	9
3.8	Компиляция и выполнение программы simpleid2	10
3.9	Установка новых атрибутов (SetUID) и смена владельца файла . .	10
3.10	Запуск simpleid2 после установки SetUID	11
3.11	Запуск simpleid2 после установки SetGID	11
3.12	Код программы readfile.c	12
3.13	Смена владельца и прав доступа у файла readfile.c	13
3.14	Запуск программы readfile	14
3.15	Создание файла file01.txt	15
3.16	Попытка выполнить действия над файлом file01.txt от имени поль- зователя guest2	16
3.17	Удаление атрибута t (Sticky-бита) и повторение действий	17
3.18	Возвращение атрибута t (Sticky-бита)	17

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 Теоретическое введение

SetUID, SetGID и Sticky - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги.

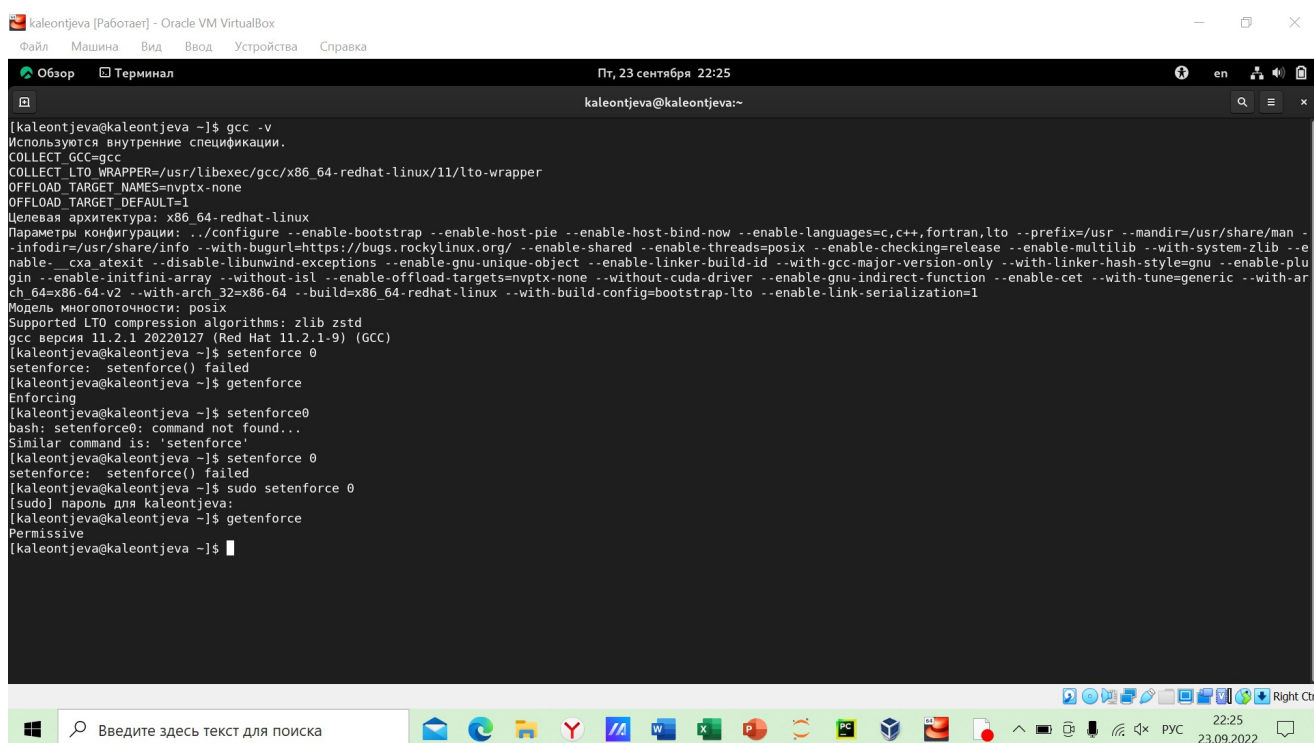
- SetUID (set user ID upon execution — «установка ID пользователя во время выполнения) являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами владельца исполняемого файла.
- SetGID (set group ID upon execution — «установка ID группы во время выполнения») являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами группы исполняемого файла.
- Sticky bit в основном используется в общих каталогах, таких как /var или /tmp, поскольку пользователи могут создавать файлы, читать и выполнять их, принадлежащие другим пользователям, но не могут удалять файлы, принадлежащие другим пользователям.

Более подробно см. в [1].

3 Выполнение лабораторной работы

3.1 Создание программы

Для начала я убедилась, что компилятор gcc установлен, используя команду “gcc -v”. Затем отключила систему запретов до очередной перезагрузки системы командой “sudo setenforce 0”, после чего команда “getenforce” вывела “Permissive” (рис. 3.1).



```
kaleontjeva [Работа] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

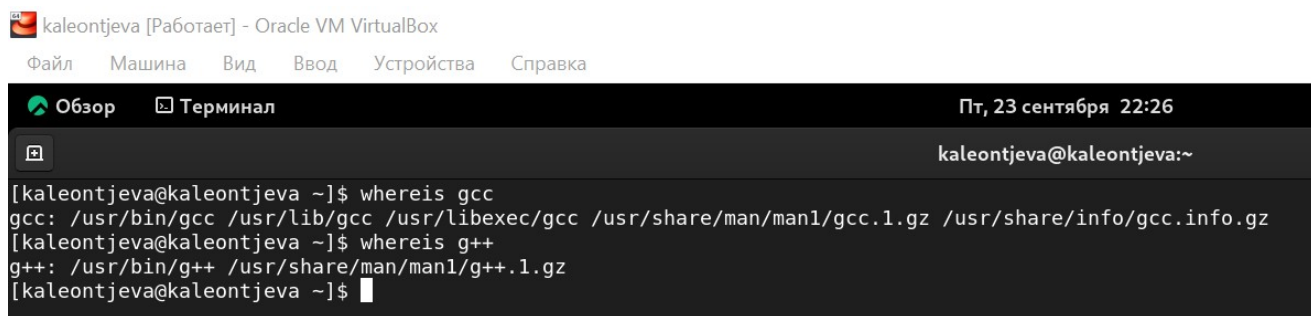
Обзор  Терминал  Пт, 23 сентября 22:25
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --enable-host-pie --enable-host-bind-now --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enable-shared --enable-threads=posix --enable-checking=release --enable-multilib --with-system-zlib --enable-cxx-exceptions --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --with-linker-hash-style=gnu --enable-plugin --enable-initfini-array --without-isl --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch=x86-64-v2 --with-arch32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-serialization=1
Модель многопоточности: posix
Supported LTO compression algorithms: zlib zstd
gcc версия 11.2.1 20220127 (Red Hat 11.2.1-9) (GCC)
[kaleontjeva@kaleontjeva ~]$ setenforce 0
setenforce: setenforce() failed
[kaleontjeva@kaleontjeva ~]$ getenforce
Enforcing
[kaleontjeva@kaleontjeva ~]$ setenforce 0
bash: setenforce0: command not found...
Similar command is: 'setenforce'
[kaleontjeva@kaleontjeva ~]$ setenforce 0
setenforce: setenforce() failed
[kaleontjeva@kaleontjeva ~]$ sudo setenforce 0
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ getenforce
Permissive
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.1: Предварительная подготовка

Проверила успешное выполнение команд “whereis gcc” и “whereis g++” (их

расположение) (рис. 3.2).



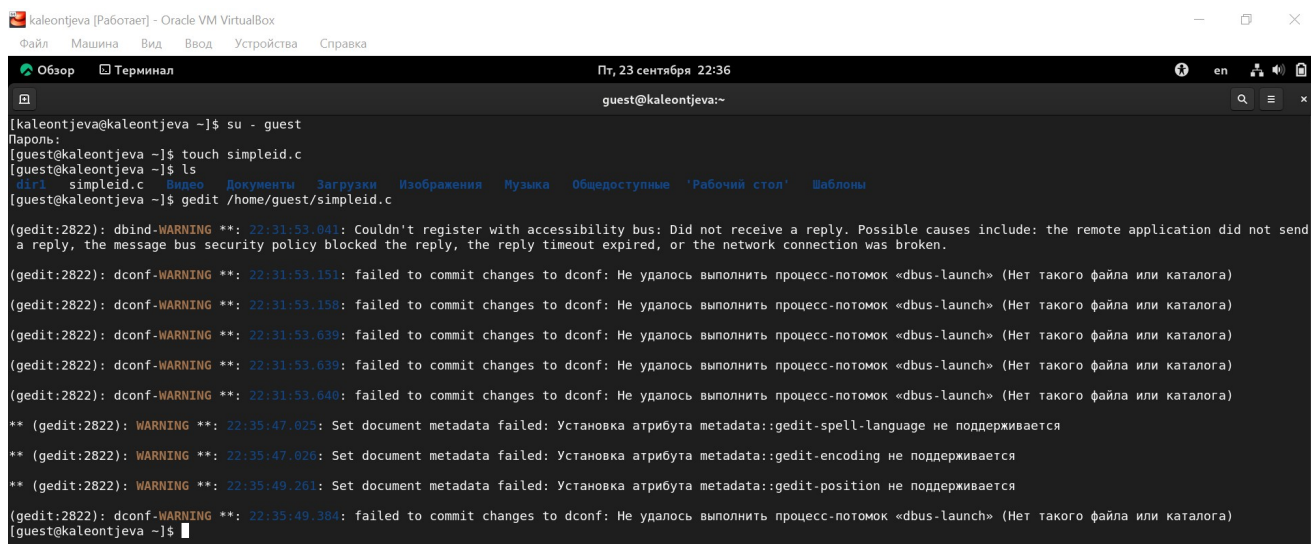
```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пт, 23 сентября 22:26
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.info.gz
[kaleontjeva@kaleontjeva ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.2: Команда “whereis”

Вошла в систему от имени пользователя guest командой “su - guest”. Создала программу simpleid.c командой “touch simpleid.c” и открыла её в редакторе командой “gedit /home/guest/simpleid.c” (рис. 3.3).



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

Обзор  Терминал  Пт, 23 сентября 22:36
guest@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ su - guest
Пароль:
[guest@kaleontjeva ~]$ touch simpleid.c
[guest@kaleontjeva ~]$ ls
dir1  simpleid.c  Видео  Документы  Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
[guest@kaleontjeva ~]$ gedit /home/guest/simpleid.c

(gedit:2822): dbind-WARNING **: 22:31:53.041: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
(gedit:2822): dconf-WARNING **: 22:31:53.151: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2822): dconf-WARNING **: 22:31:53.158: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2822): dconf-WARNING **: 22:31:53.639: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2822): dconf-WARNING **: 22:31:53.639: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2822): dconf-WARNING **: 22:31:53.640: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
** (gedit:2822): WARNING **: 22:35:47.025: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:2822): WARNING **: 22:35:47.026: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:2822): WARNING **: 22:35:49.261: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
(gedit:2822): dconf-WARNING **: 22:35:49.384: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
[guest@kaleontjeva ~]$
```

Рис. 3.3: Вход в систему и создание программы

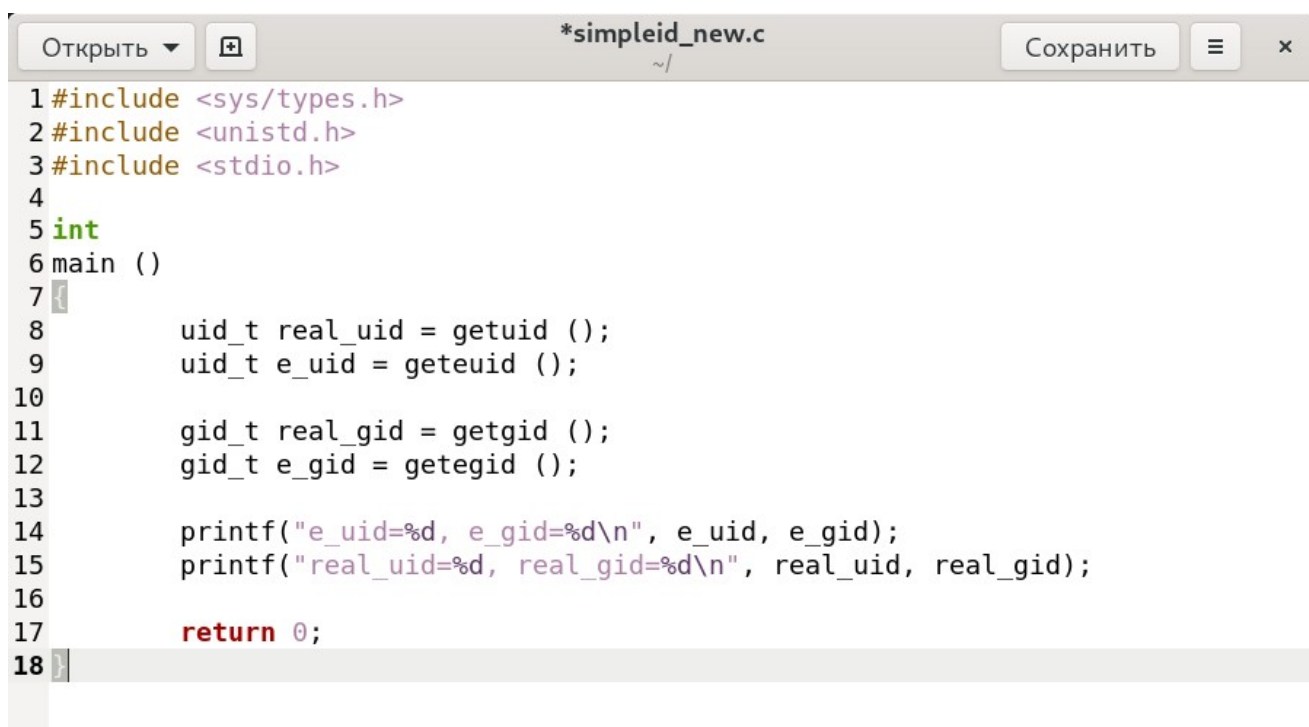
Код программы выглядит следующим образом (рис. 3.4).

Рис. 3.4: Код программы simpleid.c

Скомпилировала программу и убедилась, что файл программы был создан командой “gcc simpleid.c -o simpleid”. Выполнила программу simpleid командой “./simpleid”, а затем выполнила системную программу id командой “id”. Результаты, полученные в результате выполнения обеих команд, совпадают (uid=1001 и gid=1001) (рис. 3.5).

Рис. 3.5: Компиляция и выполнение программы simpleid

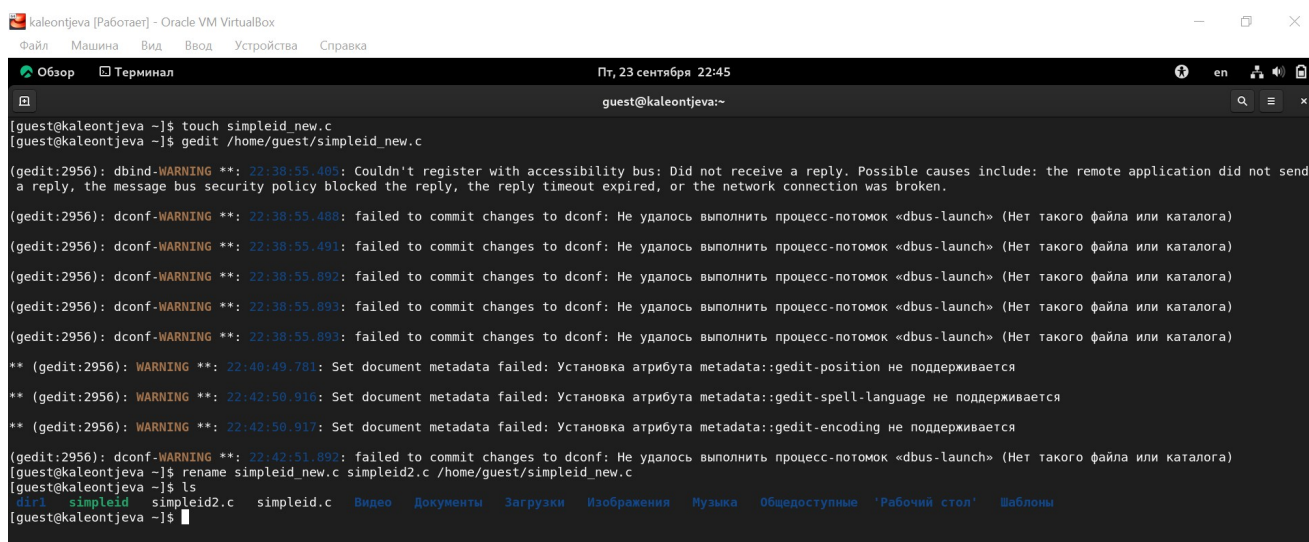
Усложнила программу, добавив вывод действительных идентификаторов (рис. 3.6).



```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t real_uid = getuid ();
9     uid_t e_uid = geteuid ();
10
11     gid_t real_gid = getgid ();
12     gid_t e_gid = getegid ();
13
14     printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
15     printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
16
17     return 0;
18 }
```

Рис. 3.6: Усложнение программы

Получившуюся программу назвала simpleid2.c (рис. 3.7).



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

Обзор  Терминал  Пт, 23 сентября 22:45
guest@kaleontjeva:~

[guest@kaleontjeva ~]$ touch simpleid_new.c
[guest@kaleontjeva ~]$ gedit /home/guest/simpleid_new.c

(gedit:2956): dbind-WARNING **: 22:38:55.409: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
(gedit:2956): dconf-WARNING **: 22:38:55.488: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2956): dconf-WARNING **: 22:38:55.491: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2956): dconf-WARNING **: 22:38:55.892: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2956): dconf-WARNING **: 22:38:55.893: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
(gedit:2956): dconf-WARNING **: 22:38:55.893: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
** (gedit:2956): WARNING **: 22:40:49.781: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
** (gedit:2956): WARNING **: 22:42:50.916: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:2956): WARNING **: 22:42:50.917: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
(gedit:2956): dconf-WARNING **: 22:42:51.892: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
[guest@kaleontjeva ~]$ ls
dir1 simpleid simpleid2.c simpleid.c Видео Документы Загрузки Изображения Музыка Общедоступные 'Рабочий стол' Шаблоны
[guest@kaleontjeva ~]$
```

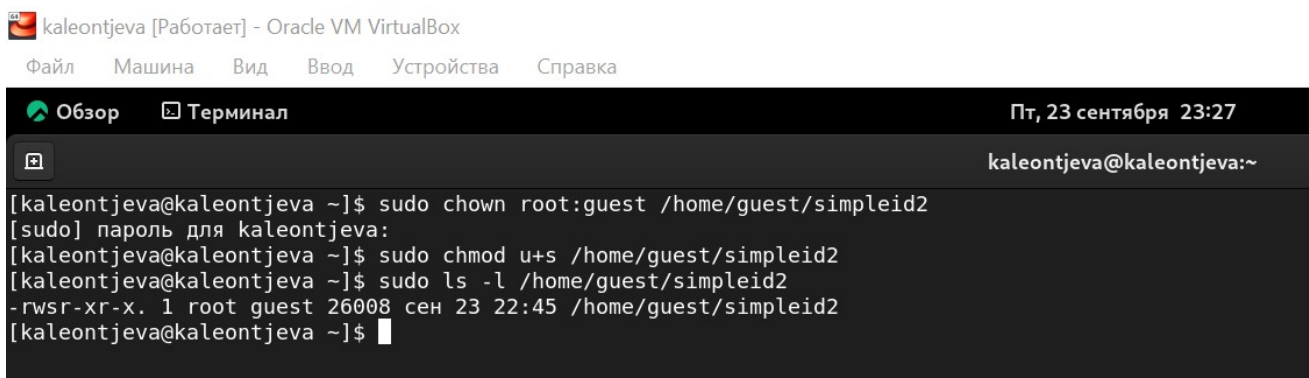
Рис. 3.7: Переименование программы в simpleid2.c

Скомпилировала и запустила simpleid2.c командами “gcc simpleid2.c -o simpleid2” и “./simpleid2” (рис. 3.8).

```
[guest@kaleontjeva ~]$ gcc simpleid2.c -o simpleid2
[guest@kaleontjeva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kaleontjeva ~]$
```

Рис. 3.8: Компиляция и выполнение программы simpleid2

От имени суперпользователя выполнила команды “sudo chown root:guest /home/guest/simpleid2” и “sudo chmod u+s /home/guest/simpleid2”, затем выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “sudo ls -l /home/guest/simpleid2” (рис. 3.9). Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит.

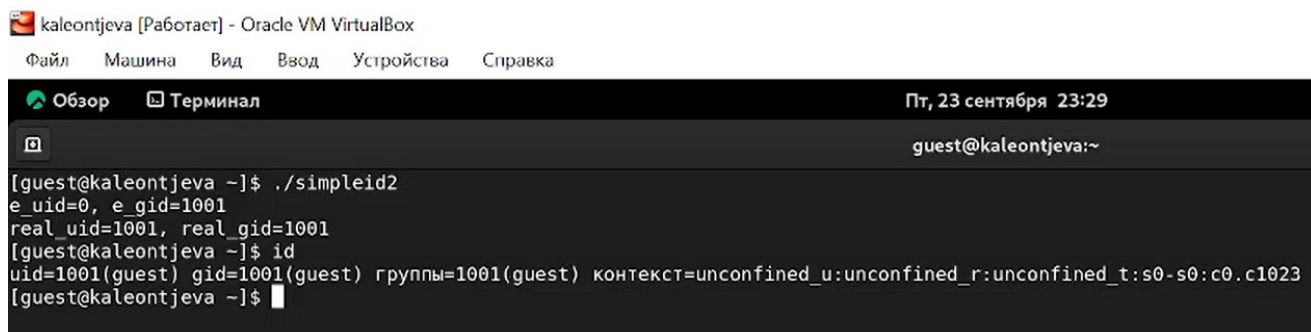


The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal has tabs for "Обзор" (Overview) and "Терминал" (Terminal), with "Терминал" selected. The terminal output shows the following commands and results:

```
kaleontjeva@kaleontjeva:~$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ sudo chmod u+s /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 26008 сен 23 22:45 /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.9: Установка новых атрибутов (SetUID) и смена владельца файла

Запустила программы simpleid2 и id. Теперь появились различия в uid (рис. 3.10).



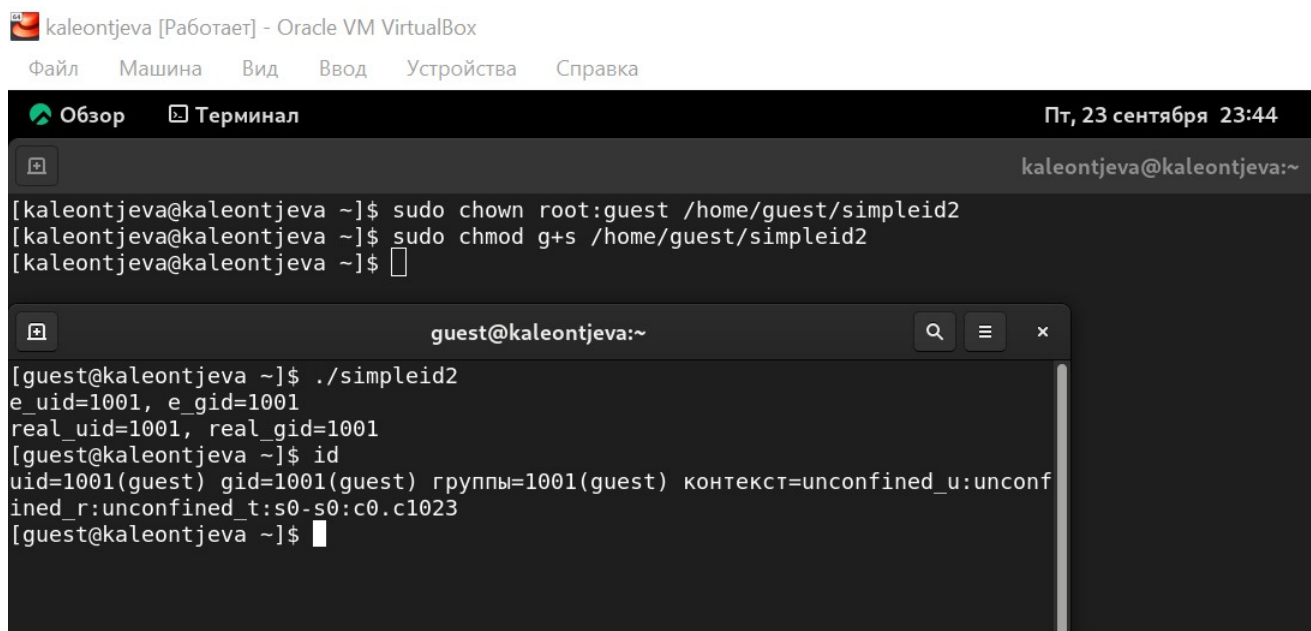
```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пт, 23 сентября 23:29
guest@kaleontjeva:~

[guest@kaleontjeva ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kaleontjeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@kaleontjeva ~]$
```

Рис. 3.10: Запуск simpleid2 после установки SetUID

Проделала тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом (рис. 3.11).



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

Обзор  Терминал  Пт, 23 сентября 23:44
kaleontjeva@kaleontjeva:~

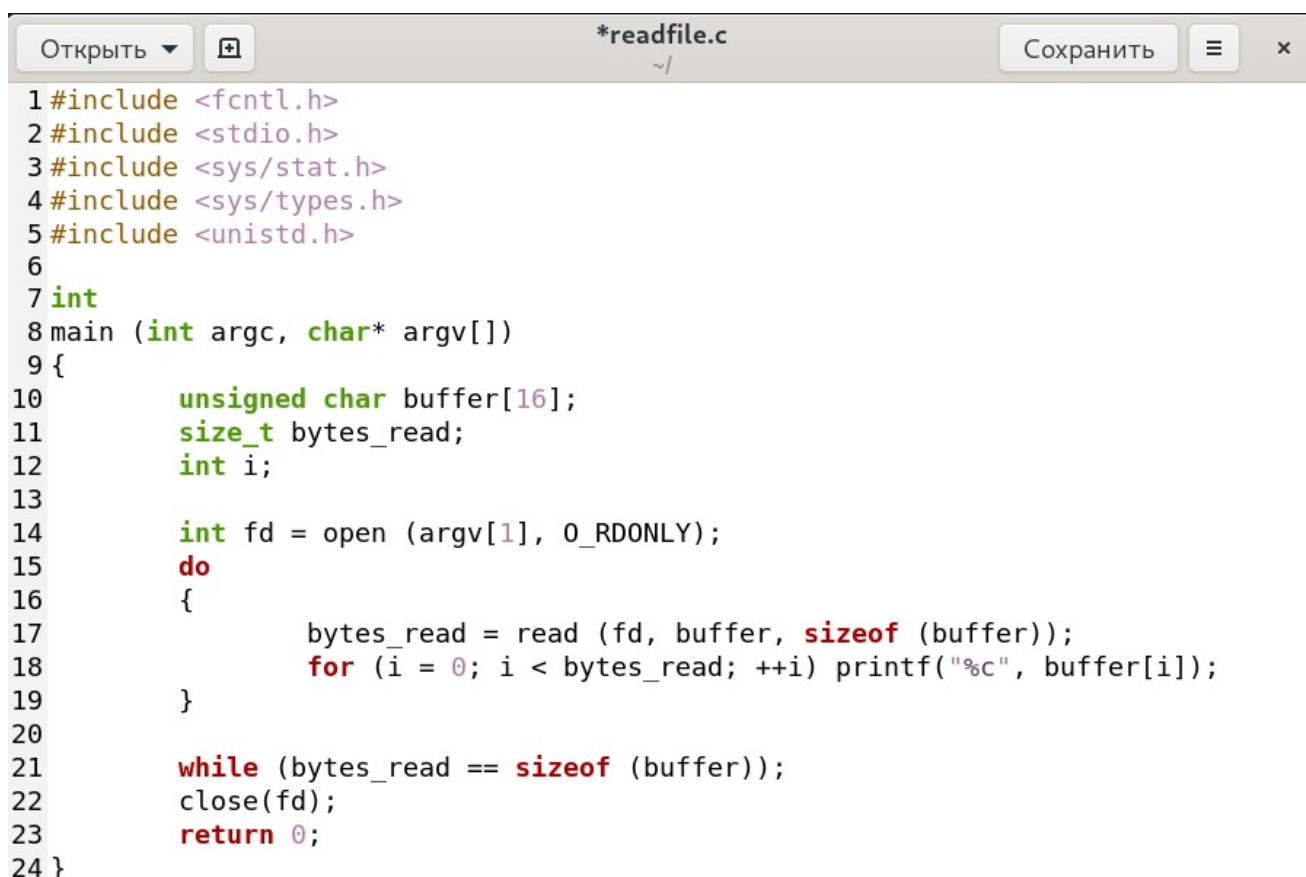
[kaleontjeva@kaleontjeva ~]$ sudo chown root:guest /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$ sudo chmod g+s /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$

guest@kaleontjeva:~

[guest@kaleontjeva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kaleontjeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@kaleontjeva ~]$
```

Рис. 3.11: Запуск simpleid2 после установки SetGID

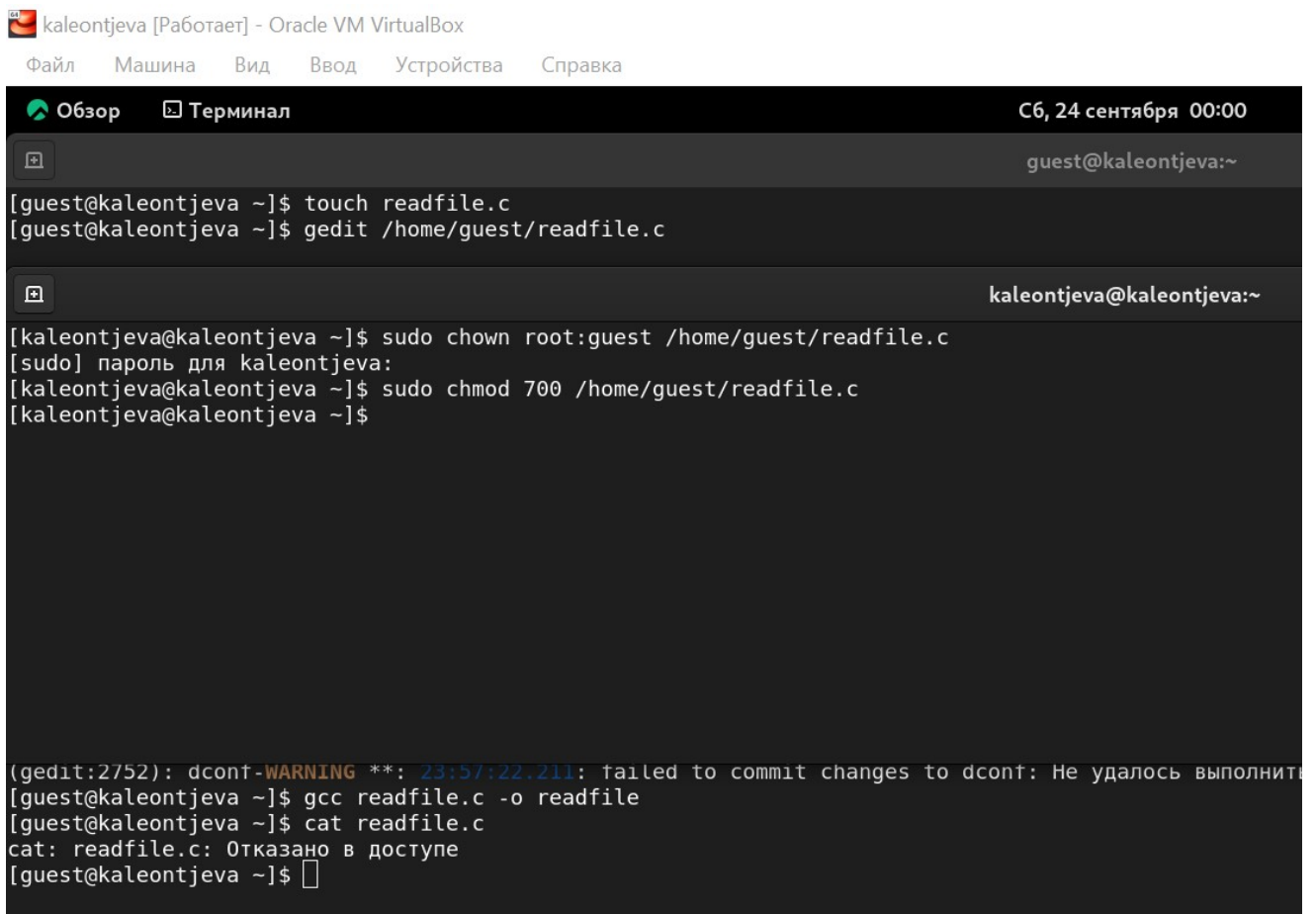
Создаем программу readfile.c (рис. 3.12).



```
1#include <fcntl.h>
2#include <stdio.h>
3#include <sys/stat.h>
4#include <sys/types.h>
5#include <unistd.h>
6
7int
8main (int argc, char* argv[])
9{
10    unsigned char buffer[16];
11    size_t bytes_read;
12    int i;
13
14    int fd = open (argv[1], O_RDONLY);
15    do
16    {
17        bytes_read = read (fd, buffer, sizeof (buffer));
18        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
19    }
20
21    while (bytes_read == sizeof (buffer));
22    close(fd);
23    return 0;
24 }
```

Рис. 3.12: Код программы readfile.c

Скомпилировала созданную программу командой “gcc readfile.c -o readfile”. Сменила владельца у файла readfile.c командой “sudo chown root:guest /home/guest/readfile.c” и поменяла права так, чтобы только суперпользователь мог прочитать его, а guest не мог, с помощью команды “sudo chmod 700 /home/guest/readfile.c”. Теперь убедилась, что пользователь guest не может прочитать файл readfile.c командой “cat readfile.c”, получив отказ в доступе (рис. 3.13).



The screenshot shows a VirtualBox window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The menu bar includes "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The terminal window has a title bar with "Обзор" and "Терминал", and a timestamp "С6, 24 сентября 00:00". The terminal shows the following commands and output:

```
guest@kaleontjeva:~  
[guest@kaleontjeva ~]$ touch readfile.c  
[guest@kaleontjeva ~]$ gedit /home/guest/readfile.c  
  
kaleontjeva@kaleontjeva:~  
[kaleontjeva@kaleontjeva ~]$ sudo chown root:guest /home/guest/readfile.c  
[sudo] пароль для kaleontjeva:  
[kaleontjeva@kaleontjeva ~]$ sudo chmod 700 /home/guest/readfile.c  
[kaleontjeva@kaleontjeva ~]$  
  
(gedit:2752): dconf-WARNING **: 23:57:22.211: failed to commit changes to dconf: Не удалось выполнить  
[guest@kaleontjeva ~]$ gcc readfile.c -o readfile  
[guest@kaleontjeva ~]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@kaleontjeva ~]$
```

Рис. 3.13: Смена владельца и прав доступа у файла readfile.c

Поменяла владельца у программы readfile и установила SetUID. Проверила, может ли программа readfile прочитать файл readfile.c командой “./readfile readfile.c”. Прочитать удалось. Аналогично проверила, можно ли прочитать файл /etc/shadow. Прочитать удалось (рис. 3.14).


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

Обзор  Терминал  Сб, 24 сентября 00:11
guest@kaleontjeva:~

[guest@kaleontjeva ~]$ echo "test" > /tmp/file01.txt
[guest@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest@kaleontjeva ~]$ chmod o+rw /tmp/file01.txt
[guest@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest@kaleontjeva ~]$

kaleontjeva@kaleontjeva:~
[kaleontjeva@kaleontjeva ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 сен 24 00:04 tmp
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.15: Создание файла file01.txt

От имени пользователя guest2 попробовала прочитать файл командой “cat /tmp/file01.txt” - это удалось. Далее попыталась дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стеревав при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой “chmod g+rw /tmp/file01.txt”. От имени пользователя guest2 попробовала удалить файл - это не удастся ни в каком из случаев, возникает ошибка (рис. 3.16).

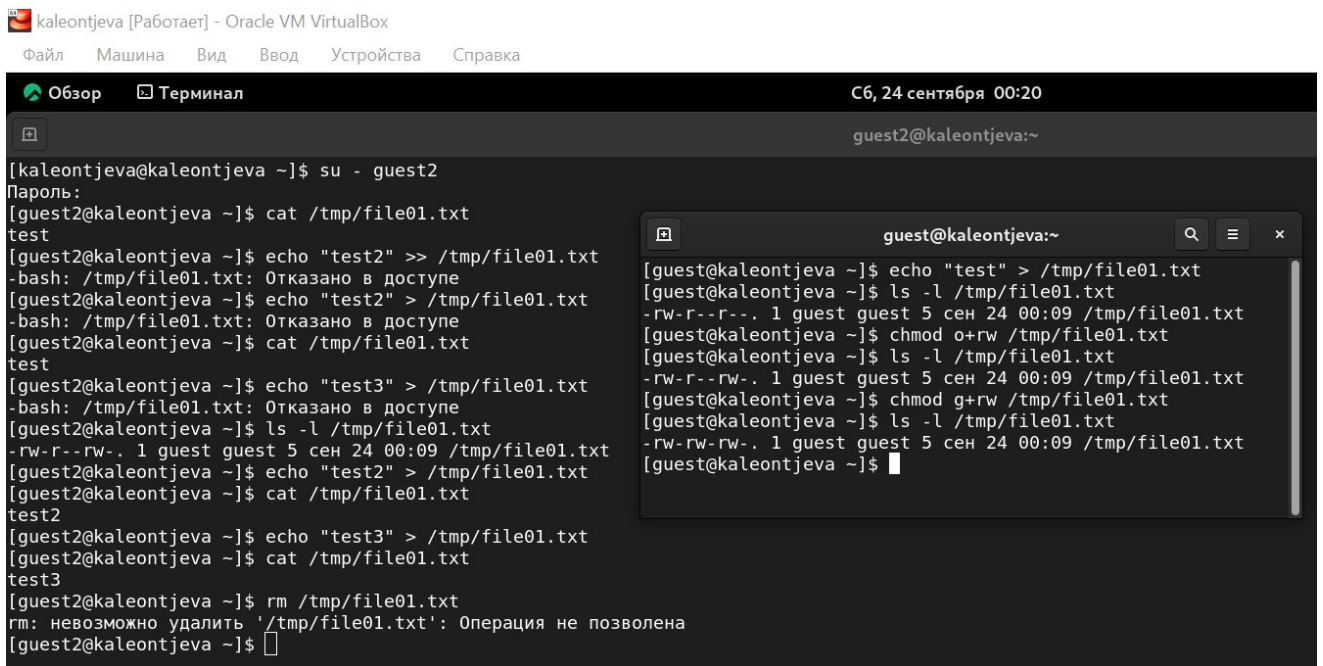


Рис. 3.16: Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

Повысила права до суперпользователя командой “su -” и выполнила команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинула режим суперпользователя командой “exit”. Повторила предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем (рис. 3.17).

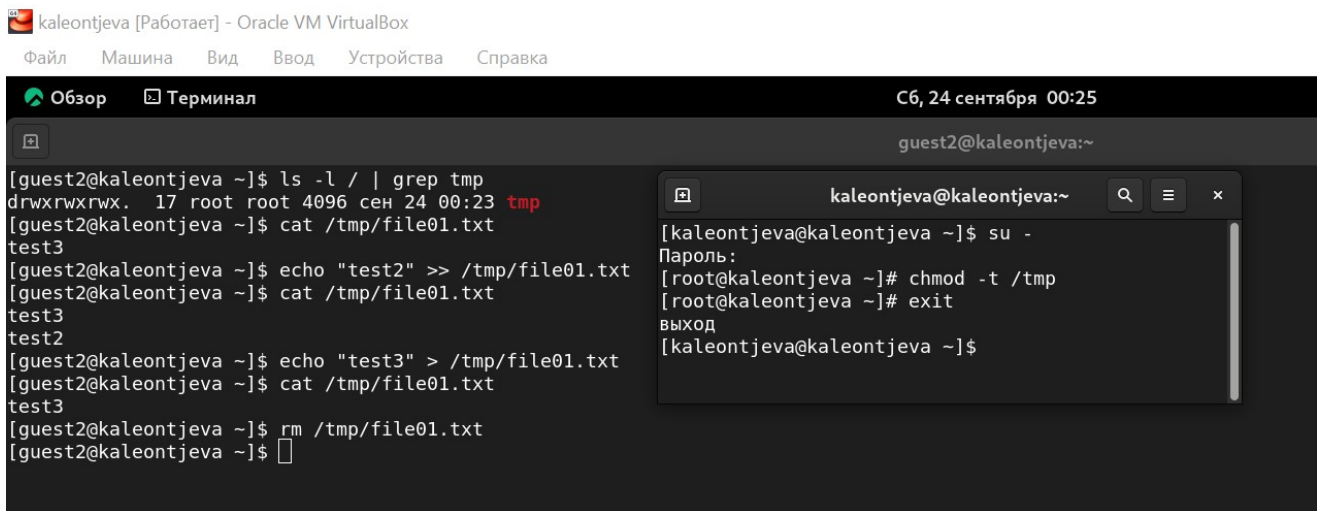


Рис. 3.17: Удаление атрибута t (Sticky-бита) и повторение действий

Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис. 3.18).

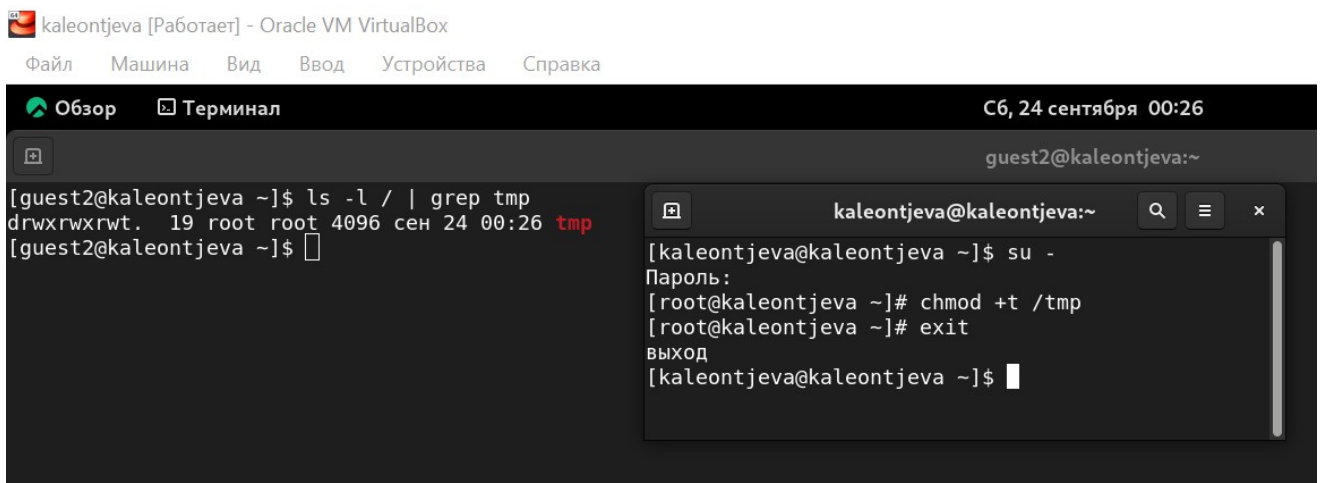


Рис. 3.18: Возвращение атрибута t (Sticky-бита)

4 Выводы

В ходе выполнения данной лабораторной работы я изучила механизмы изменения идентификаторов, применение SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

1. Стандартные права SetUID, SetGID, Sticky в Linux [Электронный ресурс].
URL: <https://linux-notes.org/standartny-e-prava-unix-suid-sgid-sticky-bity/>.