

Лабораторная работа

№ 5

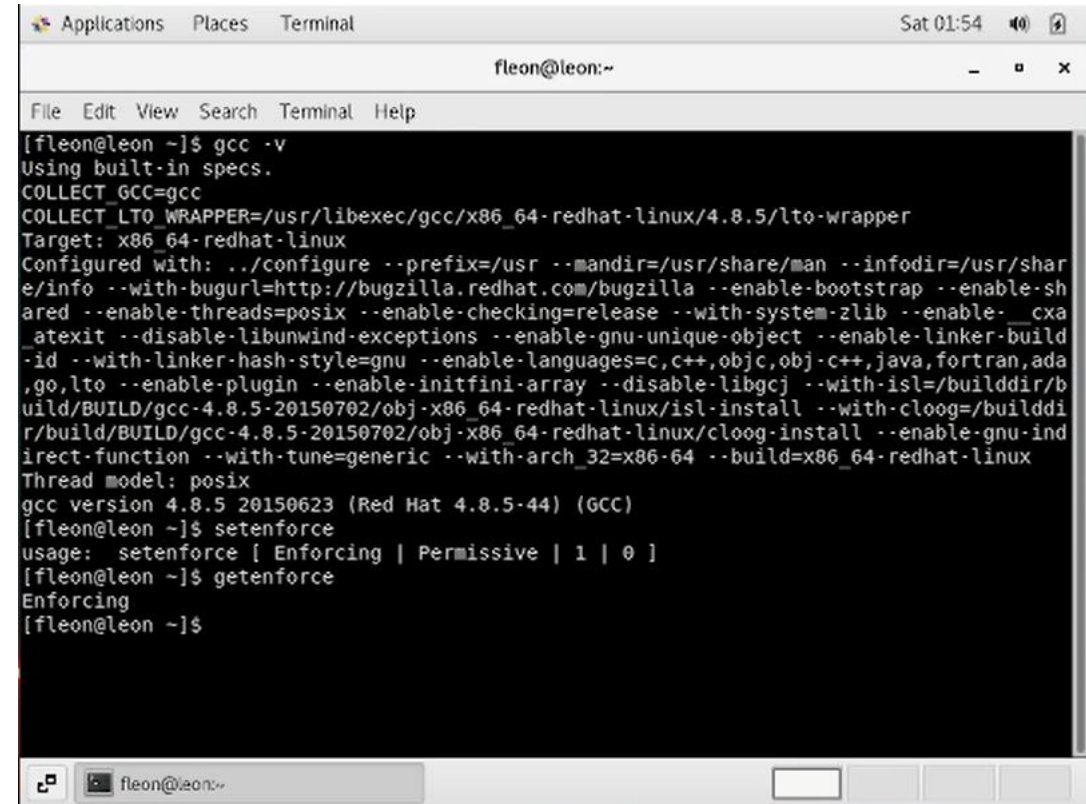
Информационная безопасность

Цель работы

Изучение механизмов модификации идентификатора, использования SetUID и Sticky bits. Получение практических навыков использования консольных команд с дополнительными атрибутами. Изучается работа механизма изменения идентификатора пользовательского процесса, а также влияние бита Sticky на запись и удаление файлов.

Выполнение лабораторной работы

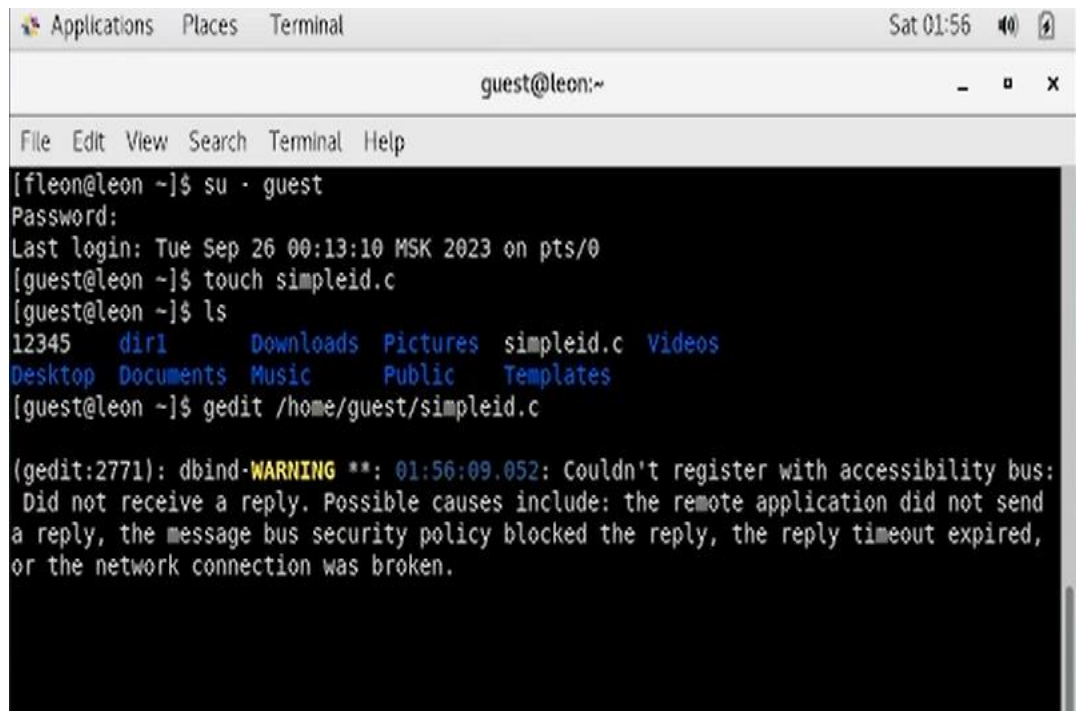
Для начала я проверил наличие компилятора gcc, используя команду 'gcc -v'. Затем я отключил системные ограничения до следующей перезагрузки системы с помощью команды "sudo setenforce 0", после чего команда "getenforce" отобразила "Разрешающий".



```
fleon@leon:~$ 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=/buildddir/build/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/isl-install --with-cloog=/buildddir/build/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)
[fleon@leon ~]$ setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
[fleon@leon ~]$ getenforce
Enforcing
[fleon@leon ~]$
```

Выполнение лабораторной работы

Я вошел в систему как пользователь "гость", используя команду "su - guest". Я создал программу под названием "simpleid.c" с помощью команды "touch simple id.c" и открыл ее в редакторе, используя команду "gedit /home/guest/simpleid.c".



```
Applications Places Terminal Sat 01:56
guest@leon:~
File Edit View Search Terminal Help
[flleon@leon ~]$ su - guest
Password:
Last login: Tue Sep 26 00:13:10 MSK 2023 on pts/0
[guest@leon ~]$ touch simpleid.c
[guest@leon ~]$ ls
12345 dirl Downloads Pictures simpleid.c Videos
Desktop Documents Music Public Templates
[guest@leon ~]$ gedit /home/guest/simpleid.c
(gedit:2771): dbind-WARNING **: 01:56:09.052: 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.
```

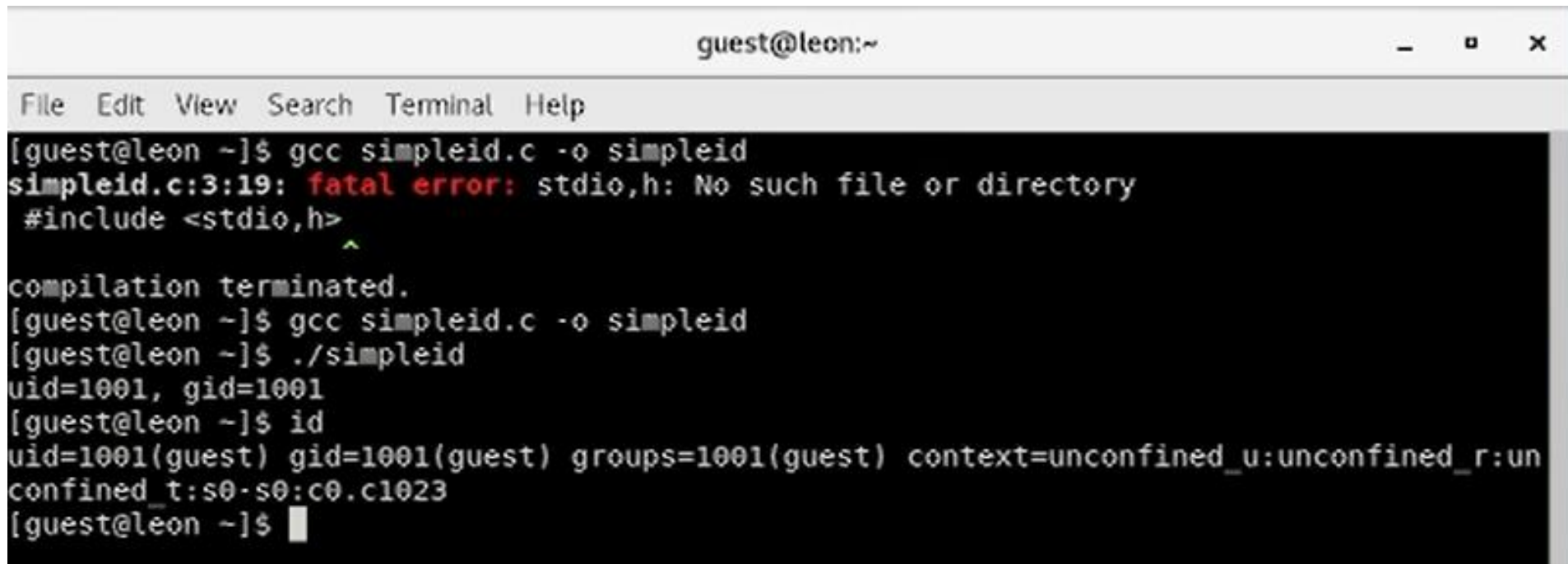


```
Applications Places Text Editor Sat 01:59
*simpleid.c
Open Save
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Выполнение лабораторной работы

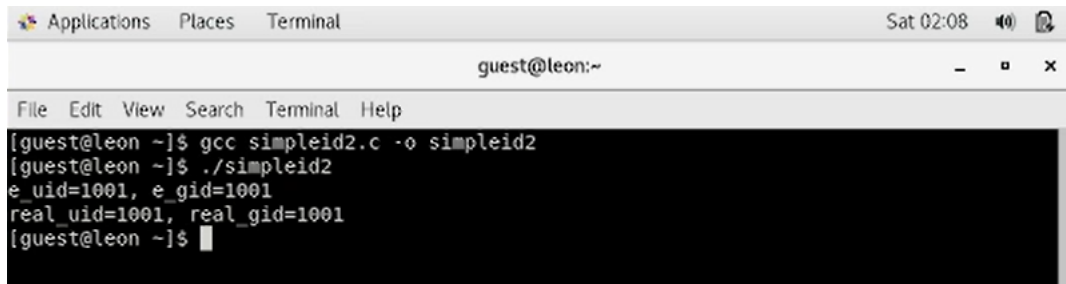
Я скомпилировал программу и убедился, что программный файл был создан с помощью команды 'gcc simplified.co simpleid'. Я выполнил программу 'simpleid' с помощью команды './simpleid', а затем запустил системную программу 'id' с помощью команды 'id'.

A screenshot of a terminal window titled 'guest@leon:~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows the following sequence of commands and output:

```
[guest@leon ~]$ gcc simpleid.c -o simpleid
simpleid.c:3:19: fatal error: stdio,h: No such file or directory
#include <stdio,h>
               ^
compilation terminated.
[guest@leon ~]$ gcc simpleid.c -o simpleid
[guest@leon ~]$ ./simpleid
uid=1001, gid=1001
[guest@leon ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@leon ~]$
```

Выполнение лабораторной работы

- Усложнил программу, добавив вывод действительных идентификаторов.
- Получившуюся программу назвала simpleid2.c
- Скомпилировала и запустила simpleid2.c командами “gcc simpleid2.c -o sipleid2” и “./simpleid2”.



```
Applications  Places  Terminal  Sat 02:08  [audio icon] [help icon]
guest@leon:~
File Edit View Search Terminal Help
[guest@leon ~]$ gcc simpleid2.c -o simpleid2
[guest@leon ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@leon ~]$
```

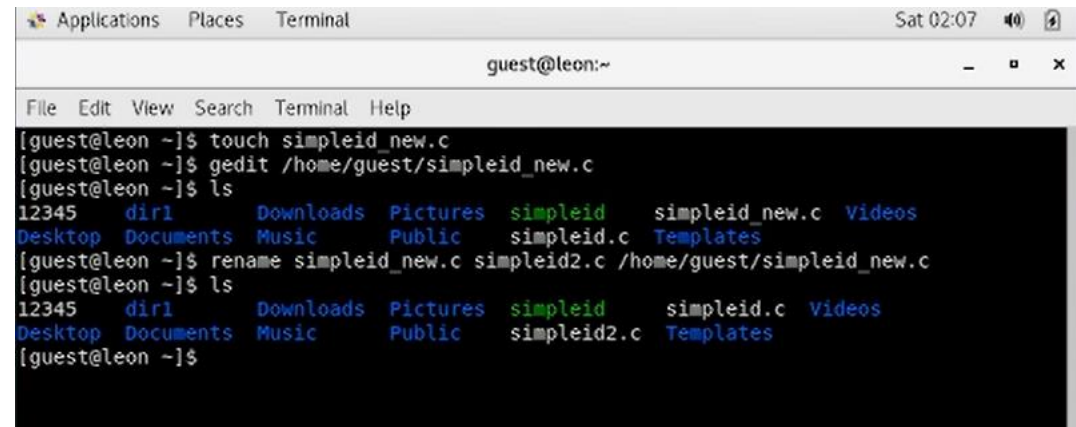


```
Applications  Places  Text Editor  Sat 02:06  [audio icon] [help icon]
simpleid_new.c
Open [icon] Save [icon] [icon] [icon] [icon]
simpleid.c  simpleid_new.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t real_uid = geteuid ();
    uid_t e_uid = geteuid ();

    gid_t real_gid = getgid ();
    gid_t e_gid = getegid();

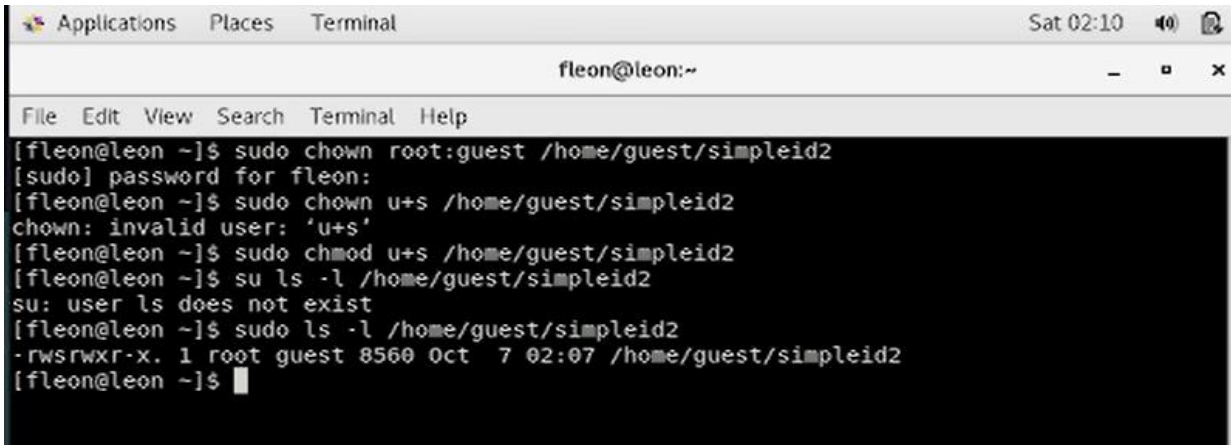
    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
    return 0;
}
```



```
Applications  Places  Terminal  Sat 02:07  [audio icon] [help icon]
guest@leon:~
File Edit View Search Terminal Help
[guest@leon ~]$ touch simpleid_new.c
[guest@leon ~]$ gedit /home/guest/simpleid_new.c
[guest@leon ~]$ ls
12345  dir1  Downloads  Pictures  simpleid  simpleid_new.c  Videos
Desktop Documents Music  Public  simpleid.c  Templates
[guest@leon ~]$ rename simpleid_new.c simpleid2.c /home/guest/simpleid_new.c
[guest@leon ~]$ ls
12345  dir1  Downloads  Pictures  simpleid  simpleid.c  Videos
Desktop Documents Music  Public  simpleid2.c  Templates
[guest@leon ~]$
```

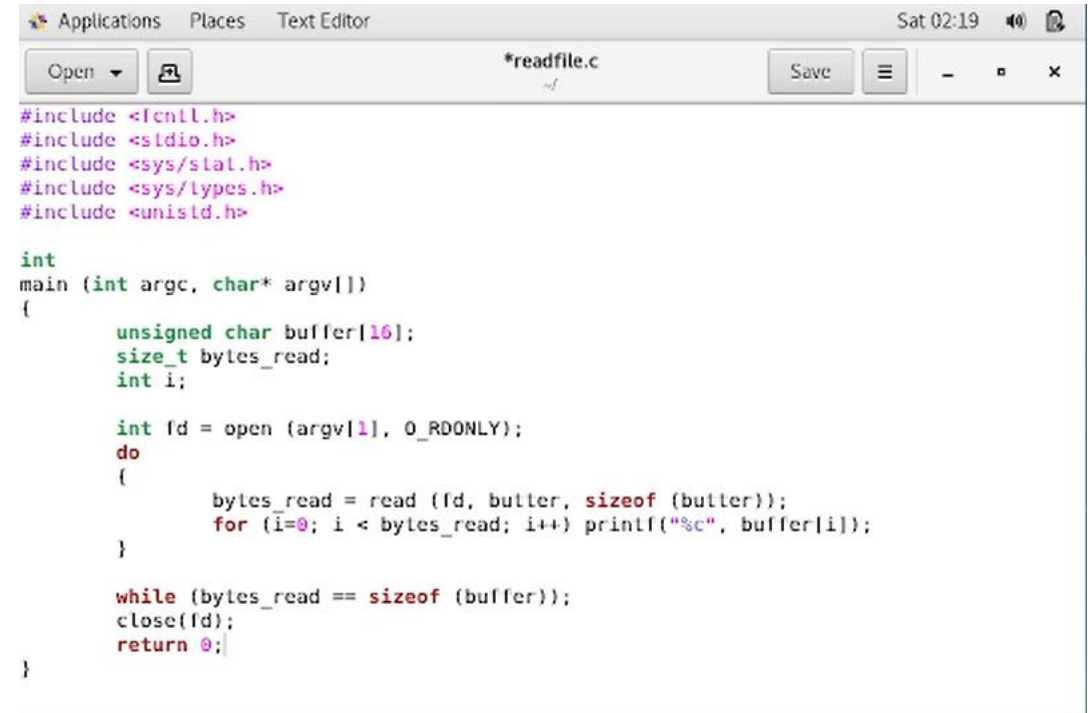
Выполнение лабораторной работы

Проделал тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом.



```
fleon@leon:~  
File Edit View Search Terminal Help  
[fleon@leon ~]$ sudo chown root:guest /home/guest/simpleid2  
[sudo] password for fleon:  
[fleon@leon ~]$ sudo chown u+s /home/guest/simpleid2  
chown: invalid user: 'u+s'  
[fleon@leon ~]$ sudo chmod u+s /home/guest/simpleid2  
[fleon@leon ~]$ su ls -l /home/guest/simpleid2  
su: user ls does not exist  
[fleon@leon ~]$ sudo ls -l /home/guest/simpleid2  
-rwsrwxr-x. 1 root guest 8560 Oct 7 02:07 /home/guest/simpleid2  
[fleon@leon ~]$
```

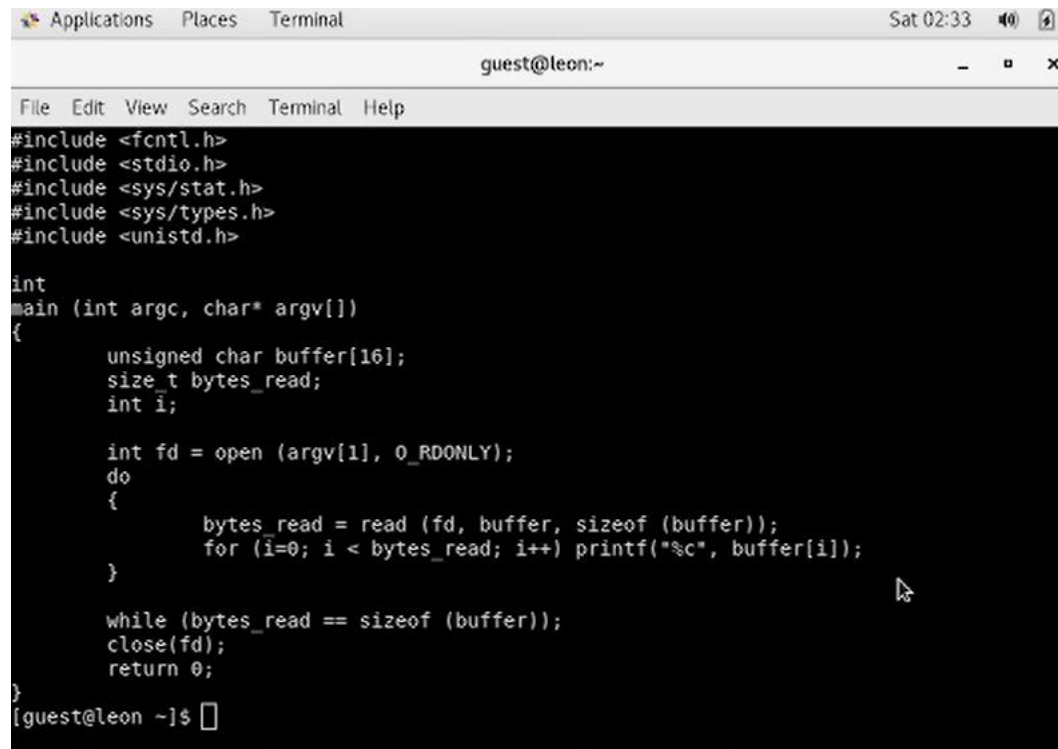
Создаем программу readfile.c



```
Applications Places Text Editor Sat 02:19  
Open *readfile.c Save  
#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;  
}
```

Выполнение лабораторной работы

Я сменил владельца программы "readfile" и установил SetUID. Я проверил, может ли программа "readfile" прочитать файл "read file.c", используя команду "./readfile readfile.c". Он смог это прочитать. Аналогично, я проверил, возможно ли прочитать файл '/etc/shadow', и это также прошло успешно.

A screenshot of a terminal window titled 'Applications Places Terminal' with a status bar showing 'Sat 02:33'. The terminal window has a menu bar with 'File Edit View Search Terminal Help' and a title bar with 'guest@leon:~'. The code displayed is a C program that takes a filename as an argument and reads its contents into a buffer of 16 unsigned characters, printing each character. The code is as follows:

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

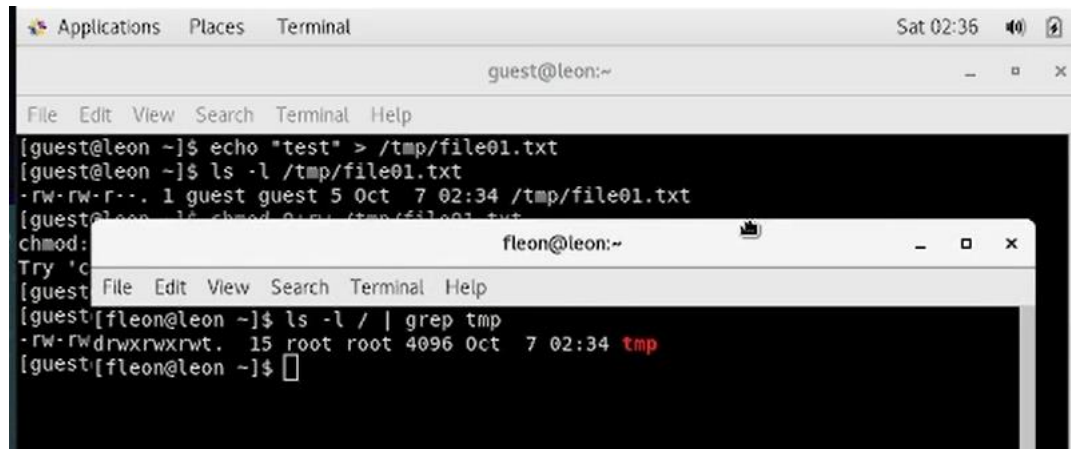
int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    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;
}
[guest@leon ~]$
```


Выполнение лабораторной работы

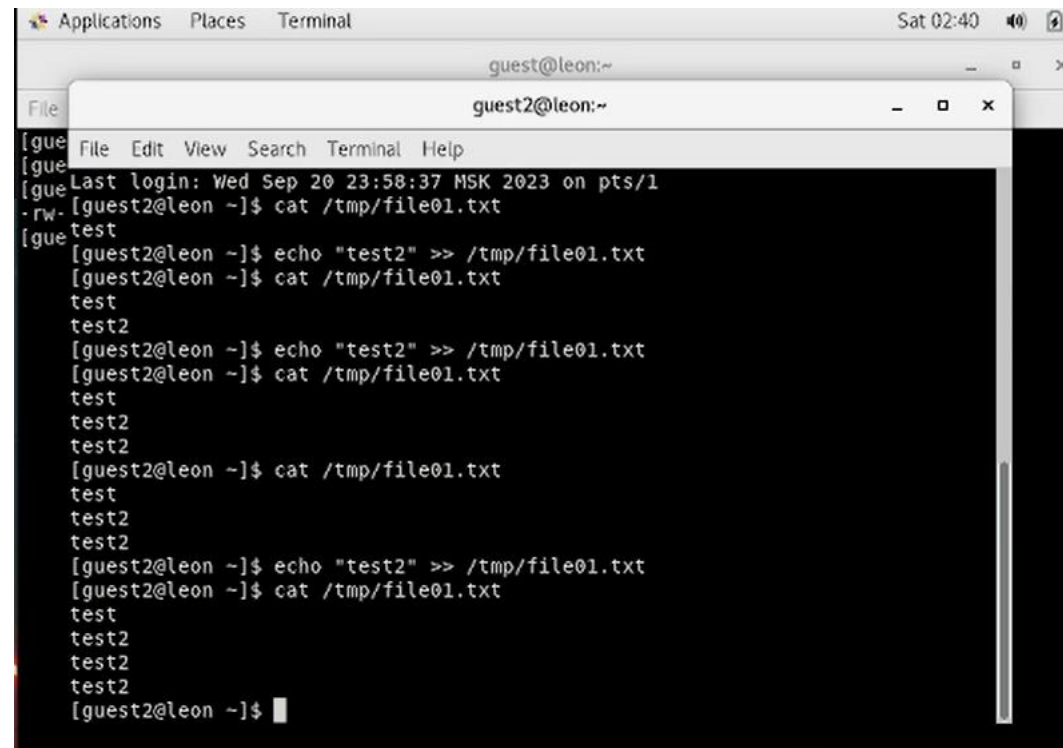
Я подтвердил, что атрибут Sticky был установлен в каталоге '/tmp', используя команду 'ls -l / | grep tmp'. От имени пользователя "гость" я создал файл с именем 'file01.txt' в каталоге '/tmp' со словом 'test' с помощью команды 'echo "test" > /tmp/file01.txt'. Я проверил атрибуты вновь созданного файла и предоставил разрешения на чтение и запись для категории пользователей "все остальные", используя команды 'ls -l /tmp/file01.txt' и 'chmod o+rw /tmp/file01.txt'.



```
Applications  Places  Terminal  Sat 02:36  [audio icon] [help icon]
guest@leon:~
File Edit View Search Terminal Help
[guest@leon ~]$ echo "test" > /tmp/file01.txt
[guest@leon ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  7 02:34 /tmp/file01.txt
[guest@leon ~]$ chmod o+rw /tmp/file01.txt
chmod:
Try 'c
[guest@leon ~]$ ls -l / | grep tmp
-rw-rwdrwxrwxrwt. 15 root root 4096 Oct  7 02:34 tmp
[guest@leon ~]$
```

Выполнение лабораторной работы

От имени пользователя "guest2" я попытался прочитать файл, используя команду "cat /tmp/file01.txt ", и это было успешно. Затем я попытался добавить слово "test2" к файлу, проверить его содержимое и записать в файл "test3", удалив при этом всю существующую информацию. Эти операции были успешными только тогда, когда я дополнительно предоставил разрешения на чтение и запись для "группы" пользователей, используя команду "chmod g+rw /tmp/file01.txt ". Однако, когда я попытался удалить файл от имени пользователя 'guest2', это не было возможно ни в одном из случаев, и произошла ошибка.



```
Applications  Places  Terminal  Sat 02:40
guest@leon:~
File Edit View Search Terminal Help
guest2@leon:~
Last login: Wed Sep 20 23:58:37 MSK 2023 on pts/1
[guest2@leon ~]$ cat /tmp/file01.txt
test
[guest2@leon ~]$ echo "test2" >> /tmp/file01.txt
[guest2@leon ~]$ cat /tmp/file01.txt
test
test2
[guest2@leon ~]$ echo "test2" >> /tmp/file01.txt
[guest2@leon ~]$ cat /tmp/file01.txt
test
test2
test2
[guest2@leon ~]$ cat /tmp/file01.txt
test
test2
test2
[guest2@leon ~]$ echo "test2" >> /tmp/file01.txt
[guest2@leon ~]$ cat /tmp/file01.txt
test
test2
test2
test2
[guest2@leon ~]$
```

Выполнение лабораторной работы

Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp



A terminal window titled "Applications Places Terminal" with a status bar showing "Sat 02:43". The window title bar also includes "guest2@leon:~". The terminal content shows the user "guest2@leon" running two "ls -l / | grep tmp" commands. The first command shows "drwxrwxrwx. 15 root root 4096 Oct 7 02:42 tmp". The second command shows "drwxrwxrwt. 16 root root 4096 Oct 7 02:43 tmp", indicating a change in permissions and the addition of the sticky bit (t).

```
File Edit View Search Terminal Help
[guest2@leon ~]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 Oct 7 02:42 tmp
[guest2@leon ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct 7 02:43 tmp
[guest2@leon ~]$
```

Выводы

Во время выполнения этого лабораторного задания я изучил механизмы модификации идентификаторов, применение SetUID и Sticky bits, а также приобрел практические навыки использования консоли с дополнительными атрибутами. Я изучил работу механизма изменения идентификатора пользовательского процесса и влияние Sticky-бита на запись и удаление файлов.