

# Информационная безопасность

Презентация к лабораторной работе  
№\_05

Габриэль Тьерри

# Информация

## Докладчик

- Габриэль Тьерри
- Студент НКНбд 01-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов имени Патриса Лумумбы
- <https://github.com/tgabriel22>
- [1032204249@pfur.ru](mailto:1032204249@pfur.ru)

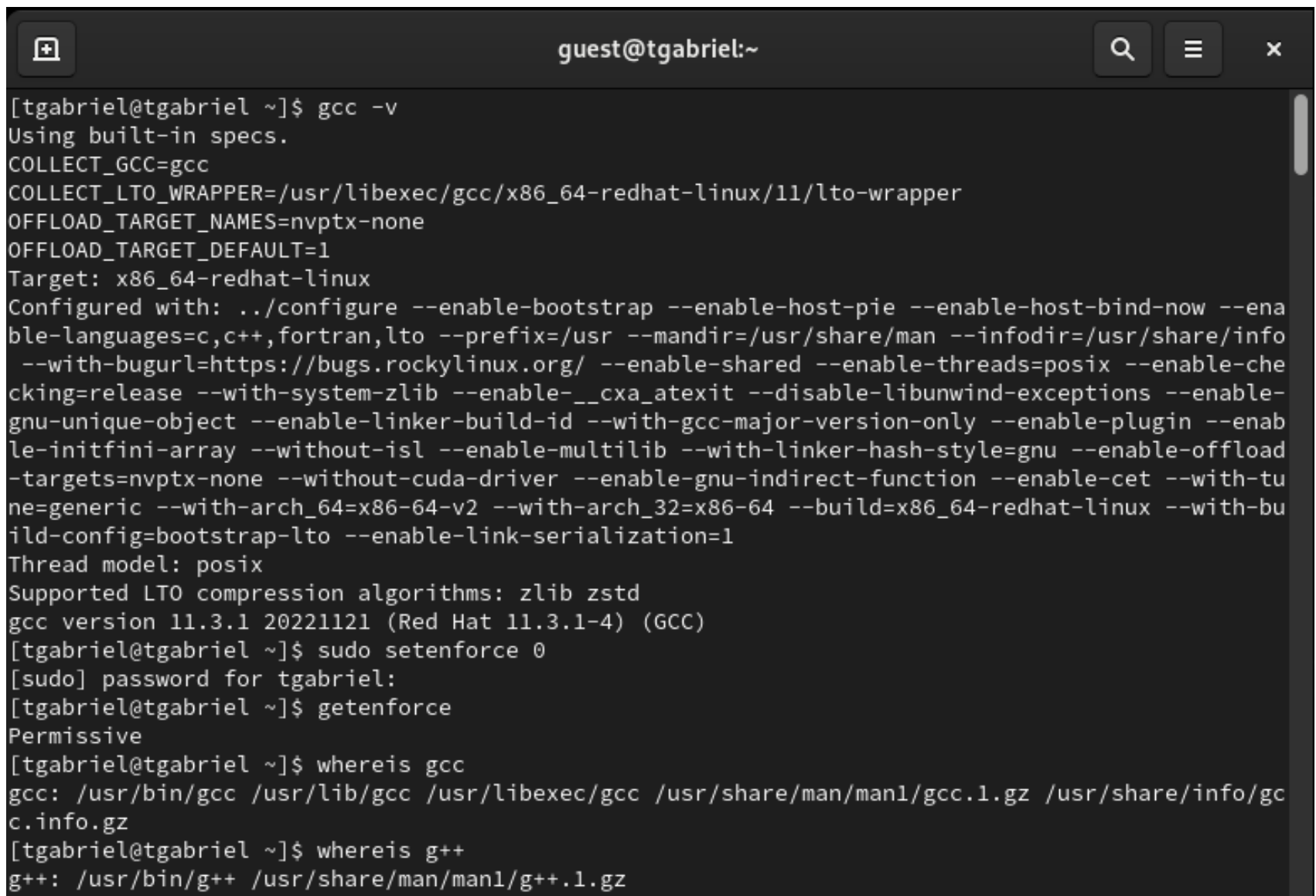
# Цель работы

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.

# Выполнение лабораторной работы

## Создание программы

- Проверил, что компилятор gcc установлен, используя команду `gcc --version`
- отключил систему запретов до очередной перезагрузка системы командой `sudo setenforce 0`, после чего команда `getenforce` вывела `Permissive`
- Проверил успешное выполнение команд `whereis gcc` и `whereis g++`

A terminal window titled 'guest@tgabriel:~' with search, menu, and close icons in the title bar. The terminal shows the output of 'gcc -v', which displays GCC version 11.3.1 configuration details for x86\_64-redhat-linux. Subsequent commands show 'sudo setenforce 0', 'sudo getenforce' returning 'Permissive', and 'whereis gcc' and 'whereis g++' showing their locations in /usr/bin and /usr/share/man.

```
[tgabriel@tgabriel ~]$ gcc -v
Using built-in specs.
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
Target: x86_64-redhat-linux
Configured with: ../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 --with-system-zlib --enable-__cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-serialization=1
Thread model: posix
Supported LTO compression algorithms: zlib zstd
gcc version 11.3.1 20221121 (Red Hat 11.3.1-4) (GCC)
[tgabriel@tgabriel ~]$ sudo setenforce 0
[sudo] password for tgabriel:
[tgabriel@tgabriel ~]$ getenforce
Permissive
[tgabriel@tgabriel ~]$ 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
[tgabriel@tgabriel ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
```

изображение 001

1. Вошел в систему от имени пользователя guest командой `su - guest`. Создал программу `simpleid.c` командой `touch simpleid.c` и открыл её в редакторе командой `vim /home/guest/simpleid.c`

```
[tgabriel@tgabriel ~]$ su - guest
Password:
[guest@tgabriel ~]$ touch simpleid.c
[guest@tgabriel ~]$ vim simpleid.c
```

изображение 002

Код программы:

```
#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;
}
```

изображение 003

3. Скомпилировал программу и убедился, что файл программы был создан командой “gcc simpleid.c -o simpleid”
4. Выполнил программу simpleid командой “./simpleid”
5. выполнил системную программу id командой “id”

```
[guest@tgabriel ~]$ gcc simpleid.c -o simpleid
[guest@tgabriel ~]$ ./simpleid
uid=1001, gid=1001
[guest@tgabriel ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

изображение 004



6. Усложнил программу, добавив вывод действительных идентификаторов

7. Скомпилировал и запустил `simpleid2.c` командами `gcc simpleid2.c -o simpleid2` и `./simpleid2`

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

изображение 005

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

изображение 006

8. От имени суперпользователя выполнил команды  
`sudo chown root:guest`  
`/home/guest/simpleid2` и `sudo chmod u+s`  
`/home/guest/simpleid2`
9. повысил временно свои права с помощью `su`.
10. выполнил проверку правильности установки  
новых атрибутов и смены владельца файла  
`simpleid2`
11. Запустил программы `simpleid2` и `id`.
12. Проделал тоже самое относительно SetGID-бита.

```
[guest@tgabriel ~]$ su
Password:
[root@tgabriel guest]# chown root:guest /home/guest/simpleid2
[root@tgabriel guest]# chmod u+s /home/guest/simpleid2
[root@tgabriel guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Oct  7 18:35 simpleid2
[root@tgabriel guest]# ./simpleid2
e_uid=%, e_gid=0
real_uid=0, real_gid=0
[root@tgabriel guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tgabriel guest]# exit
exit
[guest@tgabriel ~]$ ./simpleid2
e_uid=%, e_gid=0
real_uid=1001, real_gid=1001
[guest@tgabriel ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

изображение 007

## 13.Создал программу readfile.c

```
[guest@tgabriel ~]$ touch readfile.c
[guest@tgabriel ~]$ vim readfile.c
[guest@tgabriel ~]$ gcc readfile.c -o readfile
```

изображение 008

```
#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;
}
```

изображение 009

```
[root@tgabriel guest]# chown root -vR /home/guest/readfile.c
changed ownership of '/home/guest/readfile.c' from guest to root
[root@tgabriel guest]# ls -l
total 96
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Desktop
drwxrwxrwx. 2 guest guest   19 Sep 30 18:40 dir1
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Documents
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Downloads
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Music
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Pictures
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Public
-rwxr-xr-x. 1 guest guest 26008 Oct  7 18:54 readfile
-rw-r--r--. 1 root  guest   419 Oct  7 18:53 readfile.c
-rwxr-xr-x. 1 guest guest 25960 Oct  7 18:24 simpleid
-rwsr-xr-x. 1 root  guest 26064 Oct  7 18:35 simpleid2
-rw-r--r--. 1 guest guest   314 Oct  7 18:34 simpleid2.c
-rw-r--r--. 1 guest guest   180 Oct  7 18:22 simpleid.c
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Templates
```

изображение 010

```
[root@tgabriel guest]# chmod 700 /home/guest/readfile.c
[root@tgabriel guest]# ls -l
total 96
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Desktop
drwxrwxrwx. 2 guest guest   19 Sep 30 18:40 dir1
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Documents
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Downloads
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Music
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Pictures
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Public
-rwxr-xr-x. 1 guest guest 26008 Oct  7 18:54 readfile
-rwx-----. 1 root  guest   419 Oct  7 18:53 readfile.c
-rwxr-xr-x. 1 guest guest 25960 Oct  7 18:24 simpleid
-rwsr-xr-x. 1 root  guest 26064 Oct  7 18:35 simpleid2
-rw-r--r--. 1 guest guest   314 Oct  7 18:34 simpleid2.c
-rw-r--r--. 1 guest guest   180 Oct  7 18:22 simpleid.c
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Templates
drwxr-xr-x. 2 guest guest    6 Sep 16 16:34 Videos
```

изображение 011

```
[root@tgabriel guest]# cat 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];
    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@tgabriel guest]# exit
exit
[guest@tgabriel ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

изображение 012



## Исследование Sticky-бита

1. Выяснил, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду `ls -l / | grep tmp`
2. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test: `echo "test" > /tmp/file01.txt`
3. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: `ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt`
4. . От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt: `cat /tmp/file01.txt`
5. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2 командой `echo "test2" > /tmp/file01.txt`  
Удалось ли вам выполнить операцию? нет, не удалось.

```
[guest@tgabriel ~]$ ls -l | grep tmp
[guest@tgabriel ~]$ echo "test" > /tmp/file01.txt
[guest@tgabriel ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  7 19:49 /tmp/file01.txt
[guest@tgabriel ~]$ chmod o+rw /tmp/file01.txt
[guest@tgabriel ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  7 19:49 /tmp/file01.txt
[guest@tgabriel ~]$ su - guest2
Password:
[guest2@tgabriel ~]$ cat /tmp/file01.txt
test
[guest2@tgabriel ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@tgabriel ~]$ su - guest
Password:
[guest@tgabriel ~]$ chmod g+rw /tmp/fil01.txt
chmod: cannot access '/tmp/fil01.txt': No such file or directory
[guest@tgabriel ~]$ chmod g+rw /tmp/file01.txt
```

изображение 013

6. Проверил содержимое файла командой `cat /tmp/file01.txt`
7. От пользователя `guest2` попробовал записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt` Удалось ли вам выполнить операцию? да, удалось.
8. Проверил содержимое файла командой `cat /tmp/file01.txt`
9. От пользователя `guest2` попробовал удалить файл `/tmp/file01.txt` командой `rm /tmp/file01.txt` Удалось ли вам удалить файл? да, удалось.
10. Повысил свои права до суперпользователя следующей командой `su -` и выполнил после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`: `chmod -t /tmp`
11. Покинул режим суперпользователя командой `exit`
12. От пользователя `guest2` Проверил, что атрибута `t` у директории `/tmp` нет: `ls -l / | grep tmp`
13. Повторил предыдущие шаги. Какие наблюдаются изменения?
14. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем?
15. Повысил свои права до суперпользователя и верните атрибут `t` на директорию `/tmp`: `su - chmod +t /tmp exit`

```
[guest@tgabriel ~]$ su - guest2
Password:
[guest2@tgabriel ~]$ cat /tmp/file01.txt
test
[guest2@tgabriel ~]$ echo "test2" > /tmp/file01.txt
[guest2@tgabriel ~]$ cat /tmp/file01.txt
test2
[guest2@tgabriel ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@tgabriel ~]$ su
Password:
[root@tgabriel guest2]# exit
exit
[guest2@tgabriel ~]$ echo "test3" > /tmp/file01.txt
[guest2@tgabriel ~]$ cat /tmp/file01.txt
test3
[guest2@tgabriel ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@tgabriel ~]$ su
Password:
[root@tgabriel guest2]# chmod -t /tmp
[root@tgabriel guest2]# exit
exit
[guest2@tgabriel ~]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 Oct 7 20:27 tmp
[guest2@tgabriel ~]$ echo "test2" > /tmp/file01.txt
[guest2@tgabriel ~]$ rm /tmp/file01.txt
[guest2@tgabriel ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
[guest2@tgabriel ~]$ echo "test3" > /tmp/file01.txt
[guest2@tgabriel ~]$ cat /tmp/file01.txt
test3
[guest2@tgabriel ~]$ rm /tmp/file01.txt
[guest2@tgabriel ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
[guest2@tgabriel ~]$ exit
```

# Выводы

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.