

# **Отчёт по лабораторной работе №5**

**Дискреционное разграничение прав в Linux. Исследование влияния  
дополнительных атрибутов**

Ласурия Данил НПИбд-01-19

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	6
2.3	Исследование Sticky-бита . . . . .	9
<b>3</b>	<b>Выводы</b>	<b>14</b>
	<b>Список литературы</b>	<b>15</b>

# List of Figures

2.1	подготовка к работе . . . . .	5
2.2	программа simpleid . . . . .	6
2.3	результат программы simpleid . . . . .	6
2.4	программа simpleid2 . . . . .	7
2.5	результат программы simpleid2 . . . . .	8
2.6	программа readfile . . . . .	8
2.7	результат программы readfile . . . . .	9
2.8	исследование Sticky-бита . . . . .	12
2.9	исследование Sticky-бита . . . . .	13

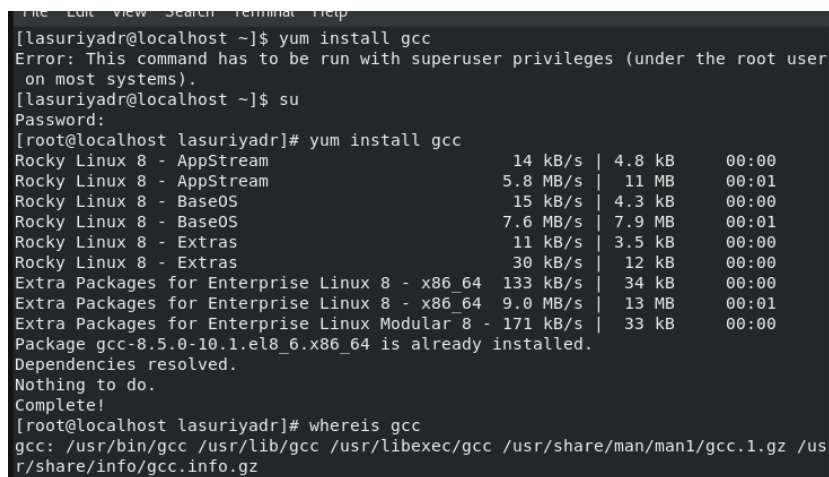
# 1 Цель работы

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

### 2.1 Подготовка

1. Для выполнения части заданий требуются средства разработки приложений. Проверили наличие установленного компилятора gcc командой `gcc -v`: компилятор обнаружен.
2. Чтобы система защиты SELinux не мешала выполнению заданий работы, отключили систему запретов до очередной перезагрузки системы командой `setenforce 0`:
3. Команда `getenforce` вывела `Permissive`:

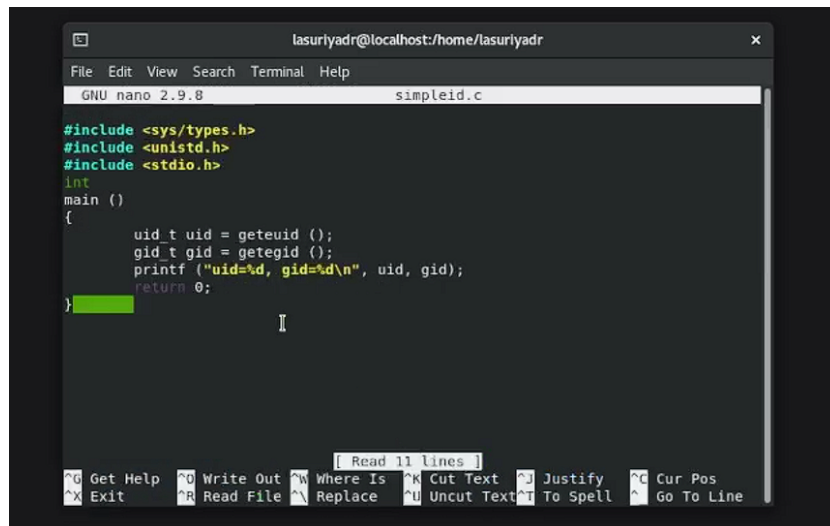


```
File Edit View Search Terminal Help
[lasuriyadr@localhost ~]$ yum install gcc
Error: This command has to be run with superuser privileges (under the root user
on most systems).
[lasuriyadr@localhost ~]$ su
Password:
[root@localhost lasuriyadr]# yum install gcc
Rocky Linux 8 - AppStream          14 kB/s | 4.8 kB      00:00
Rocky Linux 8 - AppStream          5.8 MB/s | 11 MB     00:01
Rocky Linux 8 - BaseOS             15 kB/s | 4.3 kB     00:00
Rocky Linux 8 - BaseOS             7.6 MB/s | 7.9 MB    00:01
Rocky Linux 8 - Extras             11 kB/s | 3.5 kB     00:00
Rocky Linux 8 - Extras             30 kB/s | 12 kB     00:00
Extra Packages for Enterprise Linux 8 - x86_64 133 kB/s | 34 kB     00:00
Extra Packages for Enterprise Linux 8 - x86_64 9.0 MB/s | 13 MB     00:01
Extra Packages for Enterprise Linux Modular 8 - 171 kB/s | 33 kB     00:00
Package gcc-8.5.0-10.1.el8_6.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost lasuriyadr]# whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /us
r/share/info/gcc.info.gz
```

Figure 2.1: подготовка к работе

## 2.2 Изучение механики SetUID

1. Вошли в систему от имени пользователя guest.
2. Написали программу simpleid.c.

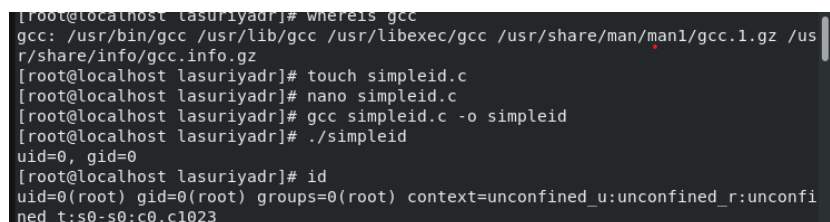


```
lasuriyadr@localhost:/home/lasuriyadr
File Edit View Search Terminal Help
GNU nano 2.9.8 simpleid.c

#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;
}
```

Figure 2.2: программа simpleid

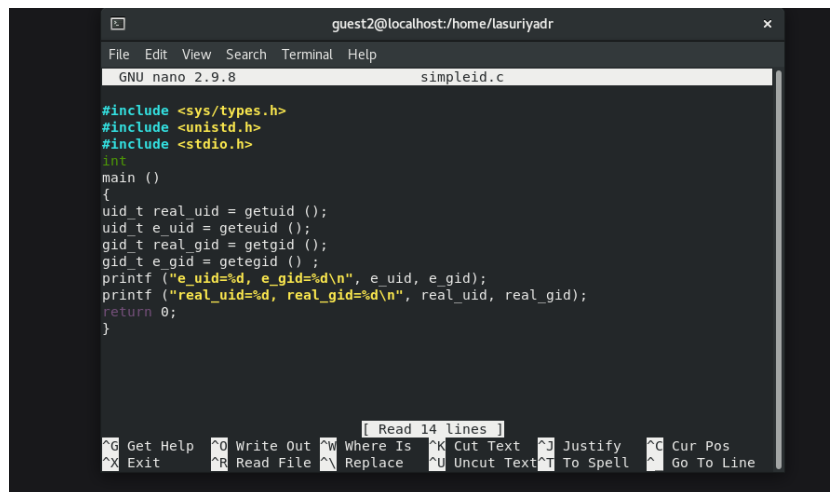
3. Скомпилировали программу и убедились, что файл программы создан: `gcc simpleid.c -o simpleid`
4. Выполнили программу simpleid командой `./simpleid`
5. Выполнили системную программу id с помощью команды `id`. uid и gid совпадает в обеих программах



```
[root@localhost lasuriyadr]# 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
[root@localhost lasuriyadr]# touch simpleid.c
[root@localhost lasuriyadr]# nano simpleid.c
[root@localhost lasuriyadr]# gcc simpleid.c -o simpleid
[root@localhost lasuriyadr]# ./simpleid
uid=0, gid=0
[root@localhost lasuriyadr]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 2.3: результат программы simpleid

6. Усложнили программу, добавив вывод действительных идентификаторов.



```
guest2@localhost:/home/tasuriyadr
File Edit View Search Terminal Help
GNU nano 2.9.8 simpleid.c

#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;
}

[ Read 14 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Figure 2.4: программа simpleid2

7. Скомпилировали и запустили simpleid2.c:

```
gcc simpleid2.c -o simpleid2
./simpleid2
```

8. От имени суперпользователя выполнили команды:

```
chown root:guest /home/guest/simpleid2
chmod u+s /home/guest/simpleid2
```

9. Использовали su для повышения прав до суперпользователя

10. Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

```
ls -l simpleid2
```

11. Запустили simpleid2 и id:

```
./simpleid2
id
```

Результат выполнения программ теперь немного отличается

12. Прodelали тоже самое относительно SetGID-бита.

```
File Edit View Search Terminal Help
[guest@localhost ~]$ nano simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
e uid=1001, e_gid=1001
real uid=1001, real gid=1001
[guest@localhost ~]$ su
Password:
su: Authentication failure
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]#
[root@localhost guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 18256 Oct  8 18:48 simpleid2
[root@localhost guest]# ./simpleid2
e uid=0, e_gid=0
real uid=0, real gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost guest]# nano readfile.c
[root@localhost guest]# gcc readfile.c -o readfile
[root@localhost guest]# chown root:root readfile
```

Figure 2.5: результат программы simpleid2

13. Написали программу readfile.c

```
guest2@localhost:/home/guest
File Edit View Search Terminal Help
GNU nano 2.9.8 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;
}
```

Figure 2.6: программа readfile

14. Откомпилировали её.



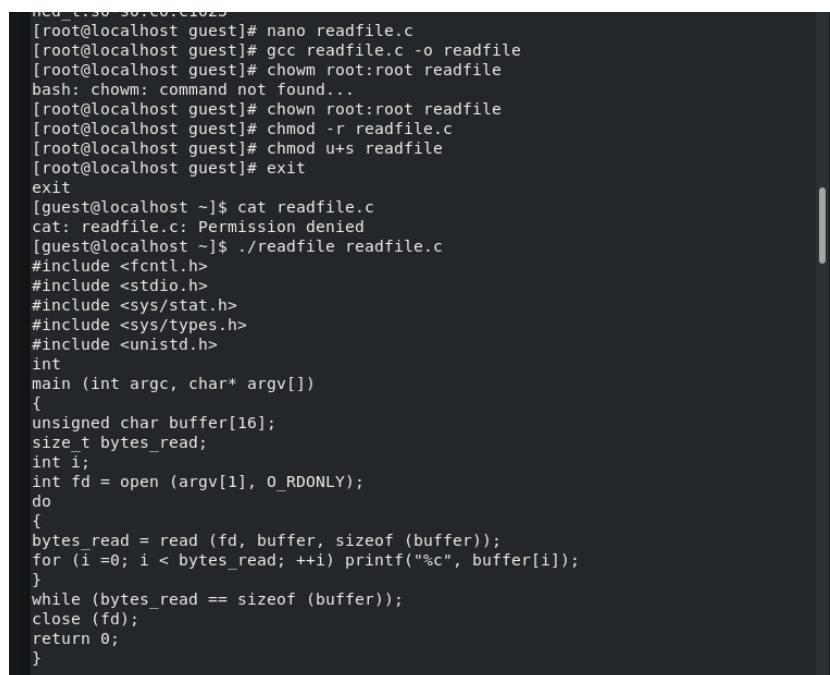
```
gcc readfile.c -o readfile
```

15. Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.

```
chown root:guest /home/guest/readfile.c
```

```
chmod 700 /home/guest/readfile.c
```

16. Проверили, что пользователь guest не может прочитать файл readfile.c.
17. Сменили у программы readfile владельца и установили SetU'D-бит.
18. Проверили, может ли программа readfile прочитать файл readfile.c
19. Проверили, может ли программа readfile прочитать файл /etc/shadow



```

[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@localhost ~]$ ./readfile 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;
}

```

Figure 2.7: результат программы readfile

## 2.3 Исследование Sticky-бита

1. Выяснили, установлен ли атрибут Sticky на директории /tmp:

```
ls -l / | grep tmp
```

2. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test:

```
echo "test" > /tmp/file01.txt
```

3. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»:

```
ls -l /tmp/file01.txt
```

```
chmod o+rw /tmp/file01.txt
```

```
ls -l /tmp/file01.txt
```

Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме «остальных пользователей».

4. От пользователя (не являющегося владельцем) попробовали прочитать файл /file01.txt:

```
cat /file01.txt
```

5. От пользователя попробовали дозаписать в файл /file01.txt слово test3 командой:

```
echo "test2" >> /file01.txt
```

6. Проверили содержимое файла командой:

```
cat /file01.txt
```

В файле теперь записано:

```
Test
```

```
Test2
```

7. От пользователя попробовали записать в файл /tmp/file01.txt слово test4, стерев при этом всю имеющуюся в файле информацию командой. Для этого воспользовалась командой `echo "test3" > /tmp/file01.txt`

8. Проверили содержимое файла командой

```
cat /tmp/file01.txt
```

9. От пользователя попробовали удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt`, однако получила отказ.

10. От суперпользователя командой выполнили команду, снимающую атрибут t (Sticky-бит) с директории /tmp:

```
chmod -t /tmp
```

Покинули режим суперпользователя командой `exit`.

11. От пользователя проверили, что атрибута t у директории /tmp нет:

```
ls -l / | grep tmp
```

12. Повторили предыдущие шаги. Получилось удалить файл

13. Удалось удалить файл от имени пользователя, не являющегося его владельцем.

14. Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp :

```
su
```

```
chmod +t /tmp
```

```
exit
```

```

[guest@localhost ~]$ cd /tmp
[guest@localhost tmp]$ echo "tst" >> file0.txt
[guest@localhost tmp]$ chmod o+rw file0.txt
[guest@localhost tmp]$ ls -l file0.txt
-rw-rw-rw-. 1 guest guest 4 Oct  8 18:54 file0.txt
[guest@localhost tmp]$ su guest2
Password:
[guest2@localhost tmp]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
[guest2@localhost tmp]$ cat file01.txt
cat: file01.txt: No such file or directory
[guest2@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
systemd-private-d1d3dd623d3b467692c032d10c883cfe-color.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fprintd.service-eDqe0b
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-nDA19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VNmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YGSGi7
tracker-extract-files.1000
[guest2@localhost tmp]$ su guest
Password:
[guest@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
systemd-private-d1d3dd623d3b467692c032d10c883cfe-color.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fprintd.service-TYUnQB
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-nDA19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VNmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YGSGi7
tracker-extract-files.1000
[guest@localhost tmp]$ su guest 2
Password:
bash: 2: No such file or directory
[guest@localhost tmp]$ su guest2
Password:
[guest2@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
systemd-private-d1d3dd623d3b467692c032d10c883cfe-color.service-YvwlZ9

```

Figure 2.8: исследование Sticky-бита

```
File Edit View Search Terminal Help
test2
[guest2@localhost tmp]$ echo "test3" > /tmp/file01.txt
[guest2@localhost tmp]$ cat /tmp/file01.txt
test3
[guest2@localhost tmp]$ echo "test2" > /tmp/file0.txt
[guest2@localhost tmp]$ ls
file01.txt
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
systemd-private-d1d3dd623d3b467692c032d10c883cfe-colord.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-nDA19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VNmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YGS6i7
tracker-extract-files.1000
[guest2@localhost tmp]$ cat file0
cat: file0: No such file or directory
[guest2@localhost tmp]$ cat file0.txt
test2
[guest2@localhost tmp]$ su chmod -t /tmp
su: invalid option -- 't'
Try 'su --help' for more information.
[guest2@localhost tmp]$ su
Password:
[root@localhost tmp]# chmod -t /tmp
[root@localhost tmp]# exit
exit
[guest2@localhost tmp]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  8 18:58 tmp
[guest2@localhost tmp]$ rm file0.txt
[guest2@localhost tmp]$ ls
file01.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
systemd-private-d1d3dd623d3b467692c032d10c883cfe-colord.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-nDA19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VNmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YGS6i7
tracker-extract-files.1000
[guest2@localhost tmp]$ rm file01.txt
[guest2@localhost tmp]$ ls
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-wDqxIi
```

Figure 2.9: исследование Sticky-бита

## 3 Выводы

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. КОМАНДА CHATTR В LINUX
2. chattr