

# **Отчёт по лабораторной работе №5**

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

Голощапова Ирина Борисовна

# Содержание

<b>1</b>	<b>Цели и задачи лабораторной работы</b>	<b>5</b>
1.1	Цели и задачи работы . . . . .	5
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
2.1	Создание программы . . . . .	6
2.2	Исследование Sticky-бита . . . . .	11
<b>3</b>	<b>Выводы</b>	<b>14</b>
<b>4</b>	<b>Библиография</b>	<b>15</b>

## Список иллюстраций

2.1	Установка gss . . . . .	6
2.2	Отключение системы запретов . . . . .	6
2.3	simpleid.c . . . . .	7
2.4	Выполнение программы simpleid . . . . .	7
2.5	simpleid2.c . . . . .	7
2.6	Запуск программы simpleid2.c . . . . .	8
2.7	Установка новых атрибутов и смена владельца simpleid2.c . . . .	8
2.8	SetGID-бит . . . . .	8
2.9	readfile.c . . . . .	9
2.10	Смена владельца readfile.c . . . . .	9
2.11	Чтение readfile.c от имени guest . . . . .	9
2.12	Смена владельца readfile.c . . . . .	10
2.13	От имени пользователя guest: readfile.c . . . . .	10
2.14	readfile.c с правами администратора . . . . .	10
2.15	/etc/shadow . . . . .	11
2.16	Наличие атрибута Sticky . . . . .	11
2.17	file01.txt . . . . .	11
2.18	Операции с file01.txt . . . . .	12
2.19	Снятие атрибута t . . . . .	12
2.20	Повторение операций над файлом . . . . .	12
2.21	Добавление атрибута t . . . . .	13

## Список таблиц

# **1 Цели и задачи лабораторной работы**

## **1.1 Цели и задачи 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 Создание программы

1. С правами администратора установила компилятор gcc (рис. 2.1)

```
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# yum install gcc
packages for the GitHub CLI      11 kB/s | 3.0 kB  00:00
packages for the GitHub CLI      3.5 kB/s | 2.6 kB  00:00
Rocky Linux 9 - BaseOS           3.5 kB/s | 4.1 kB  00:01
Rocky Linux 9 - BaseOS          989 kB/s | 1.9 MB  00:01
Rocky Linux 9 - AppStream        5.4 kB/s | 4.5 kB  00:00
Rocky Linux 9 - AppStream       2.6 MB/s | 7.1 MB  00:02
Rocky Linux 9 - Extras           2.6 kB/s | 2.9 kB  00:01
Rocky Linux 9 - Extras           9.7 kB/s | 11 kB  00:01
Пакет gcc-11.3.1-4.3.el9.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@ibgoloshchapowa guest]#
```

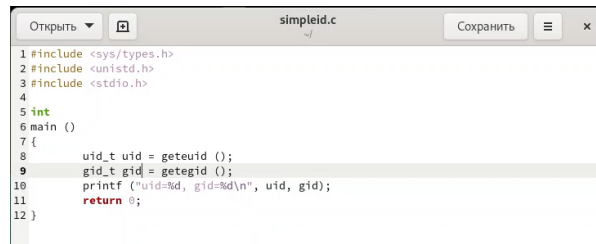
Рис. 2.1: Установка gcc

2. Отключила систему запретов до очередной перезагрузки системы командой (рис. 2.2)

```
[root@ibgoloshchapowa guest]# setenforce 0
[root@ibgoloshchapowa guest]# getenforce
Permissive
[root@ibgoloshchapowa guest]# 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@ibgoloshchapowa guest]# whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
```

Рис. 2.2: Отключение системы запретов

3. Вошла в систему от имени пользователя guest и создала программу simpleid.c со следующим кодом (рис. 2.3)



```

1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t uid = getuid ();
9     gid_t gid = getgid ();
10    printf ("uid=%d, gid=%d\n", uid, gid);
11    return 0;
12 }

```

Рис. 2.3: simpleid.c

4. Скомпилировала программу и убедилась, что файл программы создан. Далее выполнила программу simpleid и системную программу id, сравнив полученный результат (рис. 2.4)



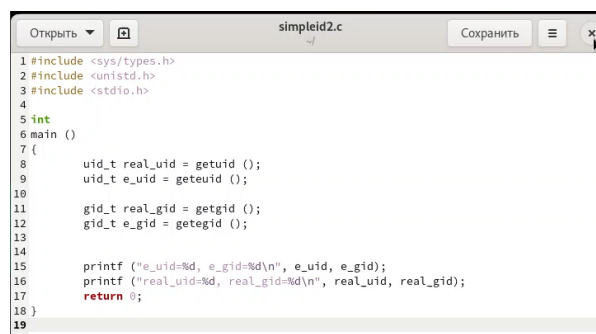
```

[guest@ibgoloshchapowa ~]$ gcc simpleid.c -o simpleid
[guest@ibgoloshchapowa ~]$ ./simpleid
uid=1001, gid=1001
[guest@ibgoloshchapowa ~]$ id
uid=1001(guest) gid=1001(guest) rpyны=1001(guest) контекст=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ibgoloshchapowa ~]$

```

Рис. 2.4: Выполнение программы simpleid

5. Усложнила программу, добавив вывод действительных идентификаторов (рис. 2.5):



```

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
15    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
16    printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
17    return 0;
18 }
19

```

Рис. 2.5: simpleid2.c

6. Скомпилировала и запустила simpleid2.c (рис. 2.6):

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

Рис. 2.6: Запуск программы simpleid2.c

7. От имени суперпользователя выполнила команды, выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2 и запустила simpleid2 и id (рис. 2.7):

```
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# chown root:guest /home/guest/simpleid2
[root@ibgoloshchapowa guest]# chmod u+s /home/guest/simpleid2
[root@ibgoloshchapowa guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 окт 5 21:26 simpleid2
[root@ibgoloshchapowa guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@ibgoloshchapowa guest]# id
uid=0(root) gid=0(root) rpnmu=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@ibgoloshchapowa guest]#
```

Рис. 2.7: Установка новых атрибутов и смена владельца simpleid2.c

8. Проделала тоже самое относительно SetGID-бита (рис. 2.8):

```
[root@ibgoloshchapowa guest]# chmod g+s /home/guest/simpleid2
[root@ibgoloshchapowa guest]# ./simpleid2
bash: ./simpleid2: Нет такого файла или каталога
[root@ibgoloshchapowa guest]# su guest
[guest@ibgoloshchapowa ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
```

Рис. 2.8: SetGID-бит

9. Создала программу readfile.c (рис. 2.9):





10. Откомпилировала её. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог (рис. 2.10).

Рис. 2.10: Смена владельца readfile.c

Проверила, что пользователь `guest` не может прочитать файл `readfile.c` (рис. 2.11):

Рис. 2.11: Чтение readfile.c от имени guest

11. Сменила у программы readfile владельца и установила SetU'D-бит (рис. 2.12).

```
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# chown root:guest /home/guest/readfile
[root@ibgoloshchapowa guest]# chmod g+s /home/guest/readfile
```

Рис. 2.12: Смена владельца readfile.c

Проверила, может ли программа readfile прочитать файл readfile.c.

Проверила, может ли программа readfile прочитать файл /etc/shadow (рис. 2.13).

- От имени пользователя guest:

```
[guest@ibgoloshchapowa ~]$ ./readfile readfile.c
bash: ./readfile: Отказано в доступе
[guest@ibgoloshchapowa ~]$ ./readfile /etc/shadow
bash: ./readfile: Отказано в доступе
```

Рис. 2.13: От имени пользователя guest: readfile.c

- С правами администратора (рис. 2.14):

```
bash: ./readfile: Отказано в доступе
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# ./readfile readfile.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

#include <fcntl.h>
#include <sys/stat.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;
}
```

Рис. 2.14: readfile.c с правами администратора

Чтение файла /etc/shadow (рис. 2.15)

```
[root@ibgoloshchapowa guest]# ./readfile /etc/shadow
root:$6Q2Z188ndN0lcsEOY$QKPLV15IqLFPu/RJIVaBHzQeBLu687L6e7V39EDzGhKXRxE093YgKYLUYwt4
bin:*:19469:0:99999:7:::
daemon:*:19469:0:99999:7:::
adm:*:19469:0:99999:7:::
lp:*:19469:0:99999:7:::
sync:*:19469:0:99999:7:::
shutdown:*:19469:0:99999:7:::
halt:*:19469:0:99999:7:::
mail:*:19469:0:99999:7:::
operator:*:19469:0:99999:7:::
games:*:19469:0:99999:7:::
ftp:*:19469:0:99999:7:::
nobody:*:19469:0:99999:7:::
systemd-coredump:!:19607:!!!!:
dbus:!:19607:!!!!:
polkitd:!:19607:!!!!: I
avahi:!:19607:!!!!:
rtkit:!:19607:!!!!:
sssd:!:19607:!!!!:
pipewire:!:19607:!!!!:
libstoragemgmt:!:19607:!!!!:
systemd-oom:!:19607:!!!!:
tss:!:19607:!!!!:

```

Рис. 2.15: /etc/shadow

## 2.2 Исследование Sticky-бита

1. Выяснила, что установлен атрибут Sticky на директории /tmp (рис. 2.16)

```
[guest@ibgoloshchapowa ~]$ ls -l / | grep tmp
drwxrwxrwt. 14 root root 4096 окт  5 22:25 tmp
[guest@ibgoloshchapowa ~]$
```

Рис. 2.16: Наличие атрибута Sticky

2. 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 для категории пользователей «все остальные» (рис. 2.17)

```
[guest@ibgoloshchapowa ~]$ echo "test" > /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт  5 22:31 /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ chmod o+rw /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт  5 22:31 /tmp/file01.txt
[guest@ibgoloshchapowa ~]$
```

Рис. 2.17: file01.txt

3. От пользователя guest2 (не являющегося владельцем) попробовала прочесть файл /tmp/file01.txt, дозаписать в файл слово test2, проверить содержимое файла, записать в файл слово test3, стерев при этом всю имеющуюся в

файле информацию командой и снова проверить содержимое файла. Затем попробовала удалить файл - не получилось (рис. 2.18)

```
[guest@ibgoloshchapowa ~]$ su guest2
Пароль:
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test
[guest2@ibgoloshchapowa guest]$ echo "test2" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test2
[guest2@ibgoloshchapowa guest]$ echo "test3" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test3
[guest2@ibgoloshchapowa guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@ibgoloshchapowa guest]$
```

Рис. 2.18: Операции с file01.txt

4. Повысила свои права до суперпользователя и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории. От пользователя guest2 проверила, что атрибута t у директории /tmp нет (рис. 2.19)

```
[guest2@ibgoloshchapowa guest]$ su -
Пароль:
[root@ibgoloshchapowa ~]# chmod -t /tmp
[root@ibgoloshchapowa ~]# exit
выход
[guest2@ibgoloshchapowa guest]$ su guest2
Пароль:
[guest2@ibgoloshchapowa guest]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 окт  5 22:35 tmp
[guest2@ibgoloshchapowa guest]$
```

Рис. 2.19: Снятие атрибута t

5. Повторила предыдущие шаги (рис. 2.20)

```
[guest2@ibgoloshchapowa guest]$ echo "test1" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test1
[guest2@ibgoloshchapowa guest]$ rm /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$
```

Рис. 2.20: Повторение операций над файлом

6. Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис. 2.21)

```
[guest2@ibgoloshchapowa guest]$ su -  
Пароль:  
[root@ibgoloshchapowa ~]# chmod +t /tmp  
[root@ibgoloshchapowa ~]# exit  
выход  
[guest2@ibgoloshchapowa guest]$
```

Рис. 2.21: Добавление атрибута t

## 3 Выводы

В ходе лабораторной работы мне удалось:

- Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
- Получить практических навыков работы в консоли с дополнительными атрибутами.
- Рассмотреть работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## 4 Библиография

1. Git - система контроля версий
2. Rocky Linux