

## Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Беличева Д. М.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- <https://dmbelicheva.github.io/ru/>

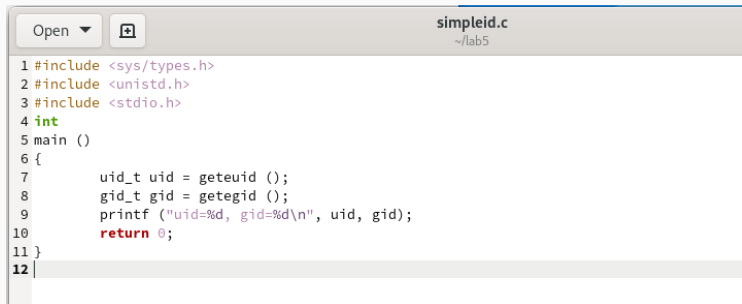


Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов.  
Получение практических навыков работы в консоли с дополнительными атрибутами.  
Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Выполнение лабораторной работы

```
gcc version 11.4.1 20221210 (Red Hat 11.4.1-6) (GCC)
[dmbelicheva@dmbelicheva ~]$ su -
Password:
[root@dmbelicheva ~]# yum install gcc
Rocky Linux 9 - BaseOS                               4.4 kB/s | 4.1 kB      00:00
Rocky Linux 9 - BaseOS                               1.1 MB/s | 2.3 MB      00:02
Rocky Linux 9 - AppStream                             4.8 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream                             2.8 MB/s | 8.0 MB      00:02
Rocky Linux 9 - Extras                               3.0 kB/s | 2.9 kB      00:00
Package gcc-11.4.1-3.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@dmbelicheva ~]# setenforce 0
[root@dmbelicheva ~]# getenforce
bash: getenforce: command not found...
[root@dmbelicheva ~]# getenforce
Permissive
[root@dmbelicheva ~]#
```

Рис. 1: Подготовка лабораторного стенда

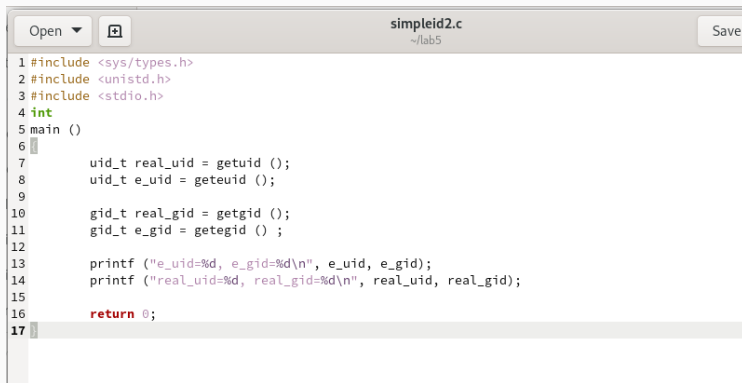


```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4 int
5 main ()
6 {
7     uid_t uid = geteuid ();
8     gid_t gid = getegid ();
9     printf ("uid=%d, gid=%d\n", uid, gid);
10    return 0;
11 }
12 |
```

Рис. 2: Содержимое файла simpleid.c

```
simpleid.c
[guest@dmbelicheva lab5]$ gcc simpleid.c -o simpleid
[guest@dmbelicheva lab5]$ ./simpleid
uid=1001, gid=1001
[guest@dmbelicheva lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@dmbelicheva lab5]$
```

Рис. 3: Запуск программы simpleid



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

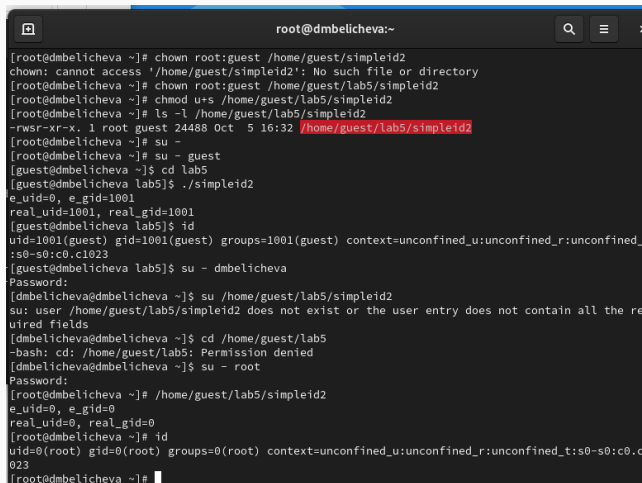
Рис. 4: Содержимое файла simpleid2.c



```
[guest@dmbelicheva lab5]$ gcc simpleid2.c -o simpleid2  
[guest@dmbelicheva lab5]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@dmbelicheva lab5]$
```

Рис. 5: Запуск программы simpleid2

## Выполнение лабораторной работы



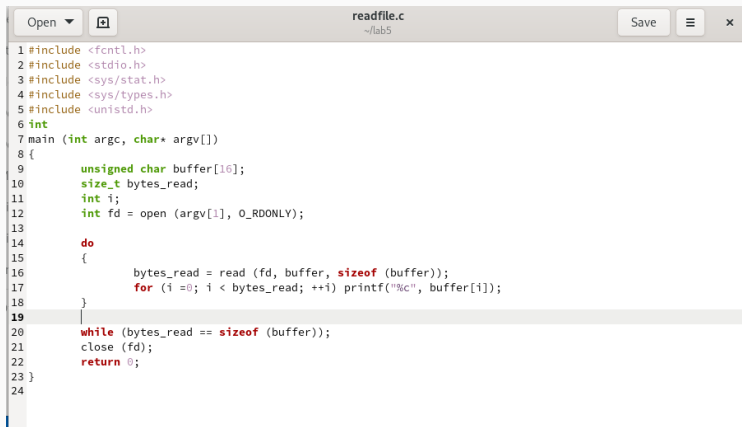
```
root@dmbelicheva:~  
[root@dmbelicheva ~]# chown root:guest /home/guest/simpleid2  
chown: cannot access '/home/guest/simpleid2': No such file or directory  
[root@dmbelicheva ~]# chown root:guest /home/guest/lab5/simpleid2  
[root@dmbelicheva ~]# chmod u+s /home/guest/lab5/simpleid2  
[root@dmbelicheva ~]# ls -l /home/guest/lab5/simpleid2  
-rwsr-xr-x. 1 root guest 24488 Oct  5 16:32 /home/guest/lab5/simpleid2  
[root@dmbelicheva ~]# su -  
[root@dmbelicheva ~]# su - guest  
[guest@dmbelicheva ~]$ cd lab5  
[guest@dmbelicheva lab5]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@dmbelicheva lab5]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_s0-s0:c0.c1023  
[guest@dmbelicheva lab5]$ su - dmbelicheva  
Password:  
[dmbelicheva@dmbelicheva ~]$ su /home/guest/lab5/simpleid2  
su: user /home/guest/lab5/simpleid2 does not exist or the user entry does not contain all the required fields  
[dmbelicheva@dmbelicheva ~]$ cd /home/guest/lab5  
-bash: cd: /home/guest/lab5: Permission denied  
[dmbelicheva@dmbelicheva ~]$ su - root  
Password:  
[root@dmbelicheva ~]# /home/guest/lab5/simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@dmbelicheva ~]# id  
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@dmbelicheva ~]#
```

Рис. 6: Изменение владельца и запуск программы simpleid2 с установленным SetUID-битом

```
[root@dmbelicheva ~]# chmod u-s /home/guest/simpleid2
chmod: cannot access '/home/guest/simpleid2': No such file or directory
[root@dmbelicheva ~]# chmod u-s /home/guest/lab5simpleid2
chmod: cannot access '/home/guest/lab5simpleid2': No such file or directory
[root@dmbelicheva ~]# chmod u-s /home/guest/lab5/simpleid2
[root@dmbelicheva ~]# chmod g+s /home/guest/lab5/simpleid2
[root@dmbelicheva ~]# ls -l /home/guest/lab5/simpleid2
-rwxr-sr-x. 1 root guest 24488 Oct  5 16:32 /home/guest/lab5/simpleid2
[root@dmbelicheva ~]# exit
logout
[dmbelicheva@dmbelicheva ~]$ su - guest
Password:
[guest@dmbelicheva ~]$ /home/guest/lab5/simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@dmbelicheva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t
:s0-s0:c0.c1023
[guest@dmbelicheva ~]$
```

Рис. 7: Запуск программы simpleid2 с установленным SetGID-битом

# Выполнение лабораторной работы



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

Рис. 8: Содержимое файла readfile.c

## Выполнение лабораторной работы

```
[guest@dmbelicheva lab5]$ gcc readfile.c -o readfile
[guest@dmbelicheva lab5]$ cat /home/guest/lab5/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;
}

[guest@dmbelicheva lab5]$ su -
Password:
[root@dmbelicheva ~]# chown root:guest /home/guest/lab5/readfile.c
[root@dmbelicheva ~]# chmod 700 /home/guest/lab5/readfile.c
```

Рис. 9: Изменение владельца и прав файла readfile.c

## Выполнение лабораторной работы

```
[root@dmbelicheva ~]# cat /home/guest/lab5/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@dmbelicheva ~]# exit
logout
[guest@dmbelicheva lab5]$ cat /home/guest/lab5/readfile.c
cat: /home/guest/lab5/readfile.c: Permission denied
[guest@dmbelicheva lab5]$
```

Рис. 10: Изменение владельца и прав файла readfile.c

## Выполнение лабораторной работы

```
[root@dmBelicheva ~]# chown root:guest /home/guest/lab5/readfile
[root@dmBelicheva ~]# chmod u+s /home/guest/lab5/readfile
[root@dmBelicheva ~]# exit
logout
[guest@dmBelicheva lab5]$ ./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;
}

[guest@dmBelicheva lab5]$ ./readfile /etc/shadow
root:$6$8rwD4MPTc6Eh5nhR$WGpqMuyr6cv2.60jI3WKs/Ld68LG00irzvJFsYMcJZ/YME6JCEff/MvEy/HSDrkEwVQcrCIS7y6rxv.PgA608::8:99999:7:::
bin:~:19820:0:99999:7:::
daemon:~:19820:0:99999:7:::
adm:~:19820:0:99999:7:::
lp:~:19820:0:99999:7:::
sync:~:19820:0:99999:7:::
busdown:~:19820:0:99999:7:::
```

Рис. 11: Установка SetUID-бита на исполняемый файл readfile и проверка прав

## Выполнение лабораторной работы

```
[guest@dmbelicheva ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  5 18:14 tmp
[guest@dmbelicheva ~]$ echo "test" > /tmp/file01.txt
[guest@dmbelicheva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  5 18:17 /tmp/file01.txt
[guest@dmbelicheva ~]$ chmod o+rw /tmp/file01.txt
[guest@dmbelicheva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  5 18:17 /tmp/file01.txt
[guest@dmbelicheva ~]$ su - guest2
Password:
[guest2@dmbelicheva ~]$ cat /tmp/file01.txt
test
[guest2@dmbelicheva ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@dmbelicheva ~]$ cat /tmp/file01.txt
test
[guest2@dmbelicheva ~]$ echo "test3" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@dmbelicheva ~]$ cat /tmp/file01.txt
test
[guest2@dmbelicheva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dmbelicheva ~]$ su -
Password:
[root@dmbelicheva ~]# chmod -t /tmp
[root@dmbelicheva ~]# exit
logout
```

Рис. 12: Исследование Sticky-бита



```
[guest2@dmbelicheva ~]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 Oct  5 18:24 tmp
[guest2@dmbelicheva ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@dmbelicheva ~]$ cat /tmp/file01.txt
test
[guest2@dmbelicheva ~]$ echo "test3" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@dmbelicheva ~]$ cat /tmp/file01.txt
test
[guest2@dmbelicheva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dmbelicheva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dmbelicheva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dmbelicheva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@dmbelicheva ~]$ su -
Password:
[root@dmbelicheva ~]# chmod +t /tmp
[root@dmbelicheva ~]# exit
logout
[guest2@dmbelicheva ~]$ ls -l / | grep tmp
```

Рис. 13: Исследование Sticky-бита

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

1. What is SUID, SGID, and Sticky Bit? [Электронный ресурс]. 2024. URL: <https://www.scaler.com/topics/special-permissions-in-linux/>.