

# Лабораторная работа №5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

---

Alexander S. Baklashov

08 October, 2022

RUDN University, Moscow, Russian Federation

## 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

---

Войдите в систему от имени пользователя guest.

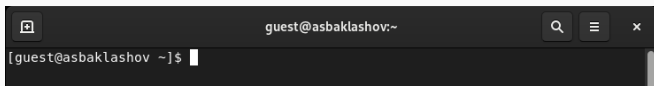


Figure 1: guest

Создайте программу simpleid.c:

```
simpleid.c      [----] 1 L:[ 1+10 11/ 11] *(174 / 174b) <EOF>
#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: simpleid.c

Скомпилируйте программу и убедитесь, что файл программы создан

```
[guest@asbaklashov Programs]$ gcc simpleid.c -o simpleid  
[guest@asbaklashov Programs]$
```

Figure 3: Скомпилируем

Выполните системную программу `id` и сравните полученный вами результат с данными предыдущего пункта задания.

```
[guest@asbaklashov Programs]$ ./simpleid
uid=1001, gid=1001
[guest@asbaklashov Programs]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@asbaklashov Programs]$
```

Figure 4: `id`

Результаты совпадают.



## Создание программы

Усложните программу, добавив вывод действительных идентификаторов.

```
simpleid2.c      [----] 1 L:[ 1+13 14/ 14] *(302 / 302b) <EOF>
#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;
}
```

Figure 5: Усложним программу

Получившуюся программу назовите simpleid2.c

Скомпилируйте и запустите simpleid2.c

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

Figure 6: simpleid2.c

От имени суперпользователя выполните команды.

```
chown root:guest /home/guest/simpleid2
```

```
chmod u+s /home/guest/simpleid2
```

1ая команда меняет владельца, 2ая - атрибуты

```
[guest@asbaklashov Programs]$ su
Password:
[root@asbaklashov Programs]# chown root:guest /home/guest/simpleid2
chown: cannot access '/home/guest/simpleid2': No such file or directory
[root@asbaklashov Programs]# chown root:guest /home/guest/Programs/simpleid2
[root@asbaklashov Programs]# chmod u+s /home/guest/Programs/simpleid2
```

Figure 7: chmod

Выполните проверку правильности установки новых атрибутов и смены владельца файла `simpleid2`

```
[root@asbaklashov Programs]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  4 18:02 simpleid2
[root@asbaklashov Programs]#
```

Figure 8: ls

Запустите simpleid2 и id

```
[root@asbaklashov Programs]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@asbaklashov Programs]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[root@asbaklashov Programs]#
```

Figure 9: id

Результаты совпадают.

Прodelайте тоже самое относительно SetGID-бита

```
[root@asbaklashov Programs]# chmod g+s /home/guest/Programs/simpleid2
[root@asbaklashov Programs]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 26008 Oct  4 18:02 simpleid2
[root@asbaklashov Programs]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@asbaklashov Programs]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@asbaklashov Programs]# exit
exit
[guest@asbaklashov Programs]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@asbaklashov Programs]$
```

Figure 10: SetGID

Создайте программу readfile.c

```
readfile.c [----] 1 L:[ 1+21 22/ 22] *(402 / 402b) <EOF>
#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 11: readfile.c

Откомпилируйте её

```
[guest@asbaklashov Programs]$ gcc readfile.c -o readfile  
[guest@asbaklashov Programs]$
```

Figure 12: Compile



## Создание программы

Смените владельца у файла `readfile.c` (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (`root`) мог прочитать его, а `guest` не мог

```
[guest@asbaklashov Programs]$ ls -l
total 96
-rwxrwxr-x. 1 guest guest 25952 Oct  4 18:15 readfile
-rw-rw-r--. 1 guest guest  402 Oct  4 18:15 readfile.c
-rwxrwxr-x. 1 guest guest 25904 Oct  4 17:58 simpleid
-rwsrwsr-x. 1 root  guest 26008 Oct  4 18:02 simpleid2
-rw-rw-r--. 1 guest guest  302 Oct  4 18:01 simpleid2.c
-rw-rw-r--. 1 guest guest  174 Oct  4 17:57 simpleid.c
[guest@asbaklashov Programs]$ su
Password:
[root@asbaklashov Programs]# chown root:guest /home/guest/Programs/readfile.c
[root@asbaklashov Programs]# chmod 700 readfile.c
[root@asbaklashov Programs]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 26008 Oct  4 18:02 simpleid2
[root@asbaklashov Programs]# ls -l readfile.c
-rwx-----. 1 root guest 402 Oct  4 18:15 readfile.c
[root@asbaklashov Programs]#
```

Figure 13: Смена владельца

Проверьте, что пользователь guest не может прочитать файл readfile.c.

```
[guest@asbaklashov Programs]$ cat readfile.c  
cat: readfile.c: Permission denied  
[guest@asbaklashov Programs]$
```

Figure 14: Проверка

Смените у программы readfile владельца и установите SetU'D-бит

```
[root@asbaklashov Programs]# chown root:guest /home/guest/Programs/readfile
[root@asbaklashov Programs]# chmod u+s /home/guest/Programs/readfile
[root@asbaklashov Programs]# ls -l
total 96
-rwsrwxr-x. 1 root  guest 25952 Oct  4 18:15 readfile
-rwx----- 1 root  guest  402 Oct  4 18:15 readfile.c
-rwxrwxr-x. 1 guest guest 25904 Oct  4 17:58 simpleid
-rwsrwsr-x. 1 root  guest 26008 Oct  4 18:02 simpleid2
-rw-rw-r--. 1 guest guest  302 Oct  4 18:01 simpleid2.c
-rw-rw-r--. 1 guest guest  174 Oct  4 17:57 simpleid.c
[root@asbaklashov Programs]#
```

Figure 15: Смена владельца

## Создание программы

Проверьте, может ли программа readfile прочитать файл readfile.c?

```
[guest@asbaklashov Programs]$ ./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;
}
```

Проверьте, может ли программа readfile прочитать файл /etc/shadow?

```
[guest@asbaklashov Programs]$ ./readfile /etc/shadow
root:$6M7vsauWmU6p9VzV$LB.gq03N6tBw0BwE/Av.XijysM8CAXPrdXtqDpI.k8l0XGG4eAQ/yaD
nJ8cxC.cjR5cGa.YgTXxvXQH1kwxS.:0:99999:7:::
bin:!:19123:0:99999:7:::
daemon:!:19123:0:99999:7:::
adm:!:19123:0:99999:7:::
lp:!:19123:0:99999:7:::
sync:!:19123:0:99999:7:::
shutdown:!:19123:0:99999:7:::
halt:!:19123:0:99999:7:::
mail:!:19123:0:99999:7:::
operator:!:19123:0:99999:7:::
games:!:19123:0:99999:7:::
ftp:!:19123:0:99999:7:::
nobody:!:19123:0:99999:7:::
systemd-coredump:!!:19240::::::
dbus:!!:19240::::::
polkitd:!!:19240::::::
rtkit:!!:19240::::::
sssd:!!:19240::::::
avahi:!!:19240::::::
pipewire:!!:19240::::::
libstoragemgmt:!!:19240::::::
tss:!!:19240::::::
geoclue:!!:19240::::::
cockpit-ws:!!:19240::::::
cockpit-wsinstance:!!:19240::::::
setroubleshoot:!!:19240::::::
flatpak:!!:19240::::::
colord:!!:19240::::::
clevis:!!:19240::::::
gdm:!!:19240::::::
systemd-oom:!:19240::::::
design:!!:19240::::::
gnome-initial-setup:!!:19240::::::
sshd:!!:19240::::::
chrony:!!:19240::::::
dnsmasq:!!:19240::::::
tcpdump:!!:19240::::::
asbaklashov:$6$EmoJr4S0E6FLAhhe$0DBZjwUW3oy9C2PATox8veYba2svR6ickpklypl17BBfh6eh
7bUnmH4pg/IQMsE7zbQtscur5wuBUGThauoA5.:0:99999:7:::
yboxaddr:!!:19240::::::
```

Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду `ls -l / | grep tmp`

Атрибут “t” установлен.

```
[guest@asbaklashov ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct  4 18:34 tmp
[guest@asbaklashov ~]$
```

Figure 18: Sticky

От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test

Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные».

```
[guest@asbaklashov ~]$ echo "test" > /tmp/file01.txt
[guest@asbaklashov ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  4 18:35 /tmp/file01.txt
[guest@asbaklashov ~]$ chmod o+rw /tmp/file01.txt
[guest@asbaklashov ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  4 18:35 /tmp/file01.txt
[guest@asbaklashov ~]$
```

Figure 19: file01.txt

## Исследование Sticky-бита

От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt

От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой

Проверьте содержимое файла командой cat /tmp/file01.txt

```
[guest@asbaklashov ~]$ su guest2
Password:
[guest2@asbaklashov guest]$ cat /tmp/file01.txt
test
[guest2@asbaklashov guest]$ echo "test2" >> /tmp/file01.txt
[guest2@asbaklashov guest]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Permission denied
[guest2@asbaklashov guest]$ cat /tmp/file01.txt
test
test2
[guest2@asbaklashov guest]$
```

Figure 20: атрибуты



От пользователя `guest2` попробуйте записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой

Проверьте содержимое файла командой `cat /tmp/file01.txt`

```
[guest2@asbaklashov guest]$ echo "test3" > /tmp/file01.txt  
[guest2@asbaklashov guest]$ cat /tmp/file01.txt  
test3  
[guest2@asbaklashov guest]$
```

Figure 21: запись в файл

От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt`

```
[guest2@asbaklashov guest]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': Operation not permitted  
[guest2@asbaklashov guest]$
```

Figure 22: удаление файла

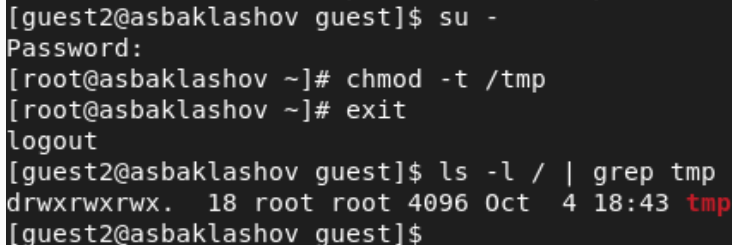
Удалить файл не удалось

## Исследование Sticky-бита

Повысьте свои права до суперпользователя следующей командой `su -` и выполните после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`: `chmod -t /tmp`

Покиньте режим суперпользователя командой `exit`

От пользователя `guest2` проверьте, что атрибута `t` у директории `/tmp` нет: `ls -l / | grep tmp`



```
[guest2@asbaklashov guest]$ su -  
Password:  
[root@asbaklashov ~]# chmod -t /tmp  
[root@asbaklashov ~]# exit  
logout  
[guest2@asbaklashov guest]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 Oct  4 18:43 tmp  
[guest2@asbaklashov guest]$
```

Figure 23: Снятие Sticky-бита

Повторим предыдущие шаги

```
[guest@asbaklashov ~]$ echo "test" > /tmp/file01.txt
[guest@asbaklashov ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  4 18:45 /tmp/file01.txt
[guest@asbaklashov ~]$ chmod o+rw /tmp/file01.txt
[guest@asbaklashov ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  4 18:45 /tmp/file01.txt
[guest@asbaklashov ~]$
```

Figure 24: шаги

```
[guest2@asbaklashov guest]$ cat /tmp/file01.txt
test
[guest2@asbaklashov guest]$ echo "test2" >> /tmp/file01.txt
[guest2@asbaklashov guest]$ cat /tmp/file01.txt
test
test2
[guest2@asbaklashov guest]$ echo "test3" > /tmp/file01.txt
[guest2@asbaklashov guest]$ cat /tmp/file01.txt
test3
[guest2@asbaklashov guest]$ rm /tmp/file01.txt
[guest2@asbaklashov guest]$
```

Figure 25: шаги

Повысьте свои права до суперпользователя и верните атрибут `t` на директорию `/tmp`

```
[guest@asbaklashov ~]$ su -  
Password:  
[root@asbaklashov ~]# chmod +t /tmp  
[root@asbaklashov ~]# exit  
logout  
[guest@asbaklashov ~]$ ls -l / | grep tmp  
drwxrwxrwt. 19 root root 4096 Oct  4 18:49 tmp  
[guest@asbaklashov ~]$
```

Figure 26: Возвращение Sticky-бита

## Выводы

---

В результате выполнения работы я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.