

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Ярметов Камран НФИбд-01-18

17 февраля, 2022, Москва, Россия

Российский Университет Дружбы Народов

## Цели и задачи

---

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

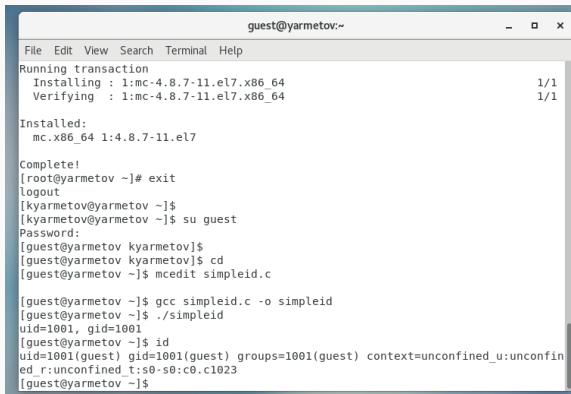
## Цель лабораторной работы

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**

---

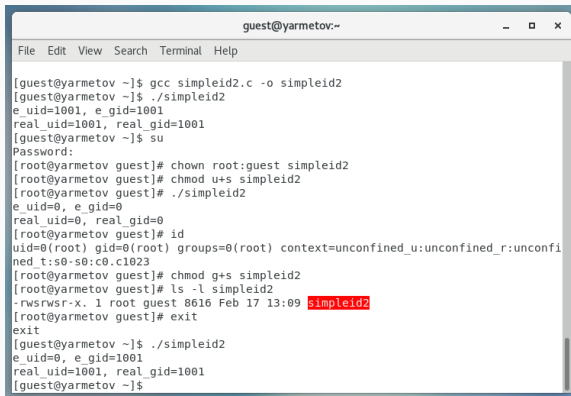
# Программа simpleid



```
guest@yarmetov:~  
File Edit View Search Terminal Help  
Running transaction  
Installing : 1:mc-4.8.7-11.el7.x86_64 1/1  
Verifying : 1:mc-4.8.7-11.el7.x86_64 1/1  
  
Installed:  
mc.x86_64 1:4.8.7-11.el7  
  
Complete!  
[root@yarmetov ~]# exit  
logout  
[kyarmetov@yarmetov ~]$  
[kyarmetov@yarmetov ~]$ su guest  
Password:  
[guest@yarmetov kyarmetov]$  
[guest@yarmetov kyarmetov]$ cd  
[guest@yarmetov ~]$ mcedit simpleid.c  
  
[guest@yarmetov ~]$ gcc simpleid.c -o simpleid  
[guest@yarmetov ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@yarmetov ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@yarmetov ~]$
```

Figure 1: результат программы simpleid

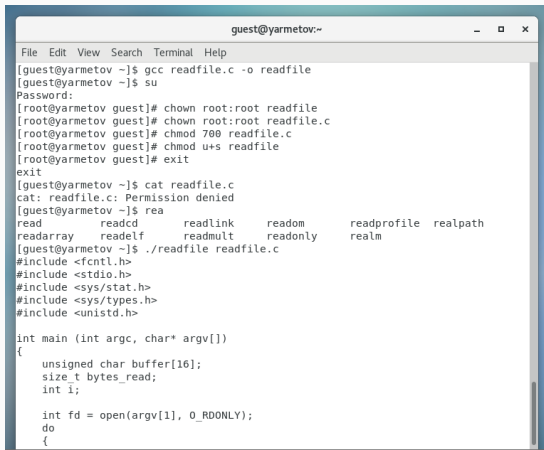
# Программа simpleid2



```
guest@yarmetov:~  
File Edit View Search Terminal Help  
[guest@yarmetov ~]$ gcc simpleid2.c -o simpleid2  
[guest@yarmetov ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@yarmetov ~]$ su  
Password:  
[root@yarmetov guest]# chown root:guest simpleid2  
[root@yarmetov guest]# chmod u+s simpleid2  
[root@yarmetov guest]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@yarmetov guest]# id  
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi  
ned_t:s0-s0:c0.c1023  
[root@yarmetov guest]# chmod g+s simpleid2  
[root@yarmetov guest]# ls -l simpleid2  
-rwsrwsr-x. 1 root guest 8616 Feb 17 13:09 simpleid2  
[root@yarmetov guest]# exit  
exit  
[guest@yarmetov ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@yarmetov ~]$
```

**Figure 2:** результат программы simpleid2

# Программа readfile

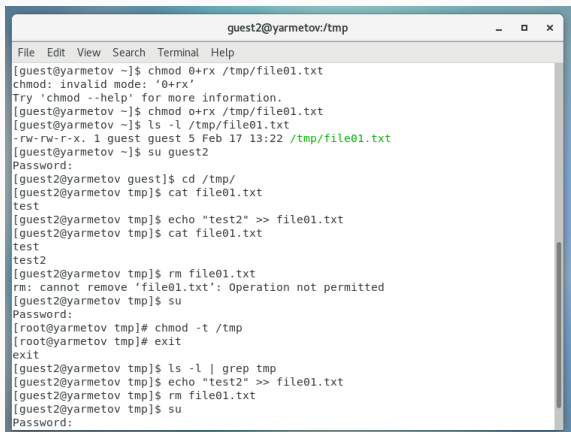


```
guest@yarmetov:~  
File Edit View Search Terminal Help  
[guest@yarmetov ~]$ gcc readfile.c -o readfile  
[guest@yarmetov ~]$ su  
Password:  
[root@yarmetov guest]# chown root:root readfile  
[root@yarmetov guest]# chown root:root readfile.c  
[root@yarmetov guest]# chmod 700 readfile.c  
[root@yarmetov guest]# chmod u+s readfile  
[root@yarmetov guest]# exit  
exit  
[guest@yarmetov ~]$ cat readfile.c  
cat: readfile.c: Permission denied  
[guest@yarmetov ~]$ read  
read          readcd      readlink      readom        readprofile   realpath  
readarray     readelf      readmult     readonly      realm  
[guest@yarmetov ~]$ ./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  
    {
```

Figure 3: результат программы readfile



# Исследование Sticky-бита



```
guest2@yarmetov:tmp
File Edit View Search Terminal Help
[guest@yarmetov ~]$ chmod 0+rx /tmp/file01.txt
chmod: invalid mode: '0+rx'
Try 'chmod --help' for more information.
[guest@yarmetov ~]$ chmod o+rx /tmp/file01.txt
[guest@yarmetov ~]$ ls -l /tmp/file01.txt
-rw-rw-r-x. 1 guest guest 5 Feb 17 13:22 /tmp/file01.txt
[guest@yarmetov ~]$ su guest2
Password:
[guest2@yarmetov guest]$ cd /tmp/
[guest2@yarmetov tmp]$ cat file01.txt
test
[guest2@yarmetov tmp]$ echo "test2" >> file01.txt
[guest2@yarmetov tmp]$ cat file01.txt
test
test2
[guest2@yarmetov tmp]$ rm file01.txt
rm: cannot remove 'file01.txt': Operation not permitted
[guest2@yarmetov tmp]$ su
Password:
[root@yarmetov tmp]# chmod -t /tmp
[root@yarmetov tmp]# exit
exit
[guest2@yarmetov tmp]$ ls -l | grep tmp
[guest2@yarmetov tmp]$ echo "test2" >> file01.txt
[guest2@yarmetov tmp]$ rm file01.txt
[guest2@yarmetov tmp]$ su
Password:
```

**Figure 4:** исследование Sticky-бита

## **Выводы**

---

## Результаты выполнения лабораторной работы

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.