

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Булаев Максим Александрович НПИбд-01-19

7 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

## 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**

---

- 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.

# Программа simpleid

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

Figure 1: результат программы simpleid

# Программа simpleid2

```
[root@abulaev guest]# chown root:guest /home/guest/simpleid2
[root@abulaev guest]# chown u+s /home/guest/simpleid2
chown: invalid user: 'u+s'
[root@abulaev guest]# chmod u+s /home/guest/simpleid2
[root@abulaev guest]# su
[root@abulaev guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  8 15:16 simpleid2
[root@abulaev guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@abulaev guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@abulaev guest]# chmod u+g /home/guest/simpleid2
[root@abulaev guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@abulaev guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  8 15:16 simpleid2
[root@abulaev guest]# chmod u-g /home/guest/simpleid2
[root@abulaev guest]# chmod g+s /home/guest/simpleid2
[root@abulaev guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@abulaev guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@abulaev guest]# touch [
```

Figure 2: результат программы simpleid2

# Программа readfile

```
[guest@mabulaev ~]$ cat readfile
cat: readfile: Permission denied
[guest@mabulaev ~]$ ./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@mabulaev ~]$ ./readfile /etc/shadow
root:$6$JRgVA4P7Ja1Abv5D$qZNRZNsGrFkdDHJl9vE0xB/D.3vKrPgu8S5ZwqyyZ0mfwNeBwQISyHkRqdeR2e
0Q6xLJUhuCM72Hs4.L4SCuV0::0:99999:7:::
```

Figure 3: результат программы readfile

# Исследование Sticky-бита

```
[guest@mabulaev tmp]$ chmod o+rw /tmp/file01.txt
[guest@mabulaev tmp]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 15:51 /tmp/file01.txt
[guest@mabulaev tmp]$ su guest2
Password:
[guest2@mabulaev tmp]$ cat /tmp/file01.txt
test
[guest2@mabulaev tmp]$ echo "test2" > /tmp/file01.txt
[guest2@mabulaev tmp]$ cat /tmp/file01.txt
test2
[guest2@mabulaev tmp]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@mabulaev tmp]$ su -
Password:
[root@mabulaev ~]# chmod -t /tmp
[root@mabulaev ~]# exit
logout
[guest2@mabulaev tmp]$ ls -l / |grep tmp
drwxrwxrwx. 15 root root 4096 Oct  8 15:56 tmp
[guest2@mabulaev tmp]$ cat /tmp/file01.txt
test2
[guest2@mabulaev tmp]$ echo "test3" > /tmp/file01.txt
[guest2@mabulaev tmp]$ cat /tmp/file01.txt
test3
[guest2@mabulaev tmp]$ rm /tmp/file01.txt
[guest2@mabulaev tmp]$ su -
Password:
[root@mabulaev ~]# chmod +t /tmp
```

Figure 4: исследование Sticky-бита



Таким образом, в ходе лабораторной работы я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получил практические навыки работы в консоли с дополнительными атрибутами, а также рассмотрел работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.