

## Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Губина О. В.

06 октября 2023

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Губина Ольга Вячеславовна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201737@pfur.ru
- <https://github.com/ovgubina>

## Вводная часть

---

- Необходимость понимания возможностей, предоставляемых различными правами и атрибутами доступа для пользователей.

- Применение SetUID-, SetGID- и Sticky-битов.

- Изучить на практике действие SetUID-, SetGID- и Sticky-битов.

- Командная строка ОС Linux



## Процесс выполнения работы

---

# Создание программы simpleid.c

```
guest@ovgubina ~]$ touch simpleid
guest@ovgubina ~]$ vim simpleid
guest@ovgubina ~]$ gcc simpleid.c -o simpleid
cc1: fatal error: simpleid.c: No such file or directory
compilation terminated.
guest@ovgubina ~]$ gcc -c simpleid
gcc: warning: simpleid: linker input file unused because linking not done
guest@ovgubina ~]$ mv simpleid simpleid.c
guest@ovgubina ~]$ gcc -c simpleid.c
guest@ovgubina ~]$ gcc simpleid.c -o simpleid
guest@ovgubina ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  simpleid  simpleid.c  simpleid.o  Templates  Videos
guest@ovgubina ~]$
```

```
guest@ovgubina:~ -- vim simpleid

#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;
}
```

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

# Программа simpleid2.c

```
guest@ovgubina:~$ vi simpleid2.c
guest@ovgubina:~$ gcc simpleid2.c -o simpleid2
guest@ovgubina:~$ ls
Desktop  Downloads  Music  Pictures  Public  simpleid  simpleid2  simpleid2.c  simpleid.o  Templates  Videos
guest@ovgubina:~$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
guest@ovgubina:~$
```

```
#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;
}
```

```
[guest@ovgubina ~]$ su ovgubina
Password:
[ovgubina@ovgubina guest]$ sudo -i
[sudo] password for ovgubina:
[root@ovgubina ~]# chown root:guest /home/guest/simpleid2
[root@ovgubina ~]# chmod u+s /home/guest/simpleid2
[root@ovgubina ~]#

[guest@ovgubina ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Oct  4 21:14 simpleid2
[guest@ovgubina ~]$
```

```
[guest@ovgubina ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@ovgubina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ovgubina ~]$
```

```
[root@ovgubina ~]# chown root:root /home/guest/simpleid2  
[root@ovgubina ~]# chmod g+s /home/guest/simpleid2  
[root@ovgubina ~]#
```

```
[guest@ovgubina ~]$ ls -l simpleid2
-rwxr-sr-x. 1 root root 26064 Oct  4 21:14 simpleid2
[guest@ovgubina ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@ovgubina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ovgubina ~]$
```



# Программа readfile.c

```
[guest@ovgubina ~]$ vim readfile.c
[guest@ovgubina ~]$ gcc readfile.c -o readfile
[guest@ovgubina ~]$
```

```
guest@ovgubina:~ — vim 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@ovgubina ~]# chown root:guest /home/guest/readfile.c  
[root@ovgubina ~]# chmod 733 /home/guest/readfile.c  
[root@ovgubina ~]#
```

```
[guest@ovgubina ~]$ ls -l readfile.c  
-rwx-wx-wx. 1 root guest 421 Oct  4 21:30 readfile.c  
[guest@ovgubina ~]$ cat readfile.c  
cat: readfile.c: Permission denied  
[guest@ovgubina ~]$
```

```
[root@ovgubina ~]# chown root:guest /home/guest/readfile  
[root@ovgubina ~]# chmod u+s /home/guest/readfile  
[root@ovgubina ~]#
```

## Попытка чтения файла readfile.c

```
[guest@ovgubina ~]$ ./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@ovgubina ~]$
```

## Попытка чтения файла /etc/shadow

```
[guest@ovgubina ~]$ ./readfile /etc/shadow
root:$6$sELndG2BtcsE5HK.$McENz/OtucocM2T7.jTwNAaa408m9H0ZJW.I0wfInQs6X/LTcQv7ph0LlgKtNGc9h7nESgphzL5XRH6R157uE0::0:99999:7:::
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:::
avahi:!!!:19607:::
rtkit:!!!:19607:::
sssd:!!!:19607:::
pipewire:!!!:19607:::
libstoragemgmt:!*:19607:::
systemd-oom:!*:19607:::
tss:!!!:19607:::
geoclue:!!!:19607:::
cockpit-ws:!!!:19607:::
cockpit-wsinstance:!!!:19607:::
flatpak:!!!:19607:::
colord:!!!:19607:::
clevis:!!!:19607:::
setroubleshoot:!!!:19607:::
gdm:!!!:19607:::
pesign:!!!:19607:::
```

```
[root@ovgubina ~]# ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  4 21:47 tmp
[root@ovgubina ~]#
```

```
[guest@ovgubina ~]$ echo "test" > /tmp/file01.txt
[guest@ovgubina ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  4 21:49 /tmp/file01.txt
[guest@ovgubina ~]$ chmod o+rw /tmp/file01.txt
[guest@ovgubina ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  4 21:49 /tmp/file01.txt
[guest@ovgubina ~]$
```

## Попытка дозаписи и записи в файл и его удаление

```
[guest@ovgubina ~]$ su guest2
Password:
[guest2@ovgubina guest]$ cat /tmp/file01.txt
test
[guest2@ovgubina guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ovgubina guest]$ cat /tmp/file01.txt
test
[guest2@ovgubina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ovgubina guest]$ cat /tmp/file01.txt
test
[guest2@ovgubina guest]$
```

```
[guest2@ovgubina guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@ovgubina guest]$
```

```
[guest2@ovgubina guest]$ su -  
Password:  
[root@ovgubina ~]# chmod -t /tmp  
[root@ovgubina ~]# exit  
logout  
[guest2@ovgubina guest]$
```



## Попытка дозаписи и записи в файл и его удаление

```
[guest2@ovgubina guest]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  4 21:54 tmp
[guest2@ovgubina guest]$ cat /tmp/file01.txt
test
[guest2@ovgubina guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ovgubina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ovgubina guest]$ cat /tmp/file01.txt
test
```

```
[guest2@ovgubina guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@ovgubina guest]$
```

## Результаты работы

---

- Изучила на практике действие SetUID-, SetGID- и Sticky-битов.

## Вывод

---

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.