

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Венчаков Никита Юрьевич¹

3 октября, 2022

¹Российский университет дружбы народов, Москва, Россия

- Венчаков Никита Юрьевич
- студент 4 курса
- Студенческий билет: 1032196697
- группа НБИбд-01-19
- Российский университет дружбы народов
- venchakov2001@gmail.com

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 битаSticky на запись и удаление файлов.

Выполнение лабораторной работы

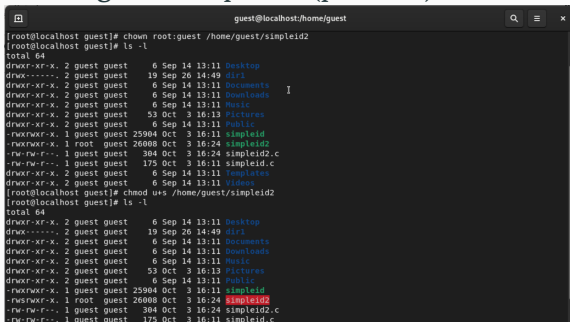
1. Создал программу simpleid.c: (рис.Nº1)

```
[guest@localhost ~]$ touch simpleid.c
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      Templates
dir      Downloads  Pictures   simpleid.c  Videos
```

2. Усложнил программу, добавив вывод действительных идентификаторов. Скомпилировал и запустил simpleid2.c: (рис. №2)

```
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public    simpleid2  simpleid.c  Videos
dirl     Downloads  Pictures   simpleid  simpleid2.c  Templates
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$
```

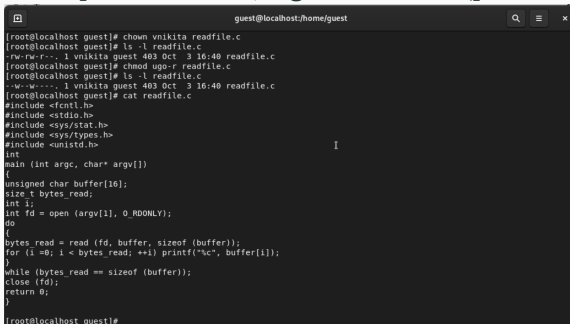
3. От имени суперпользователя выполните команды:
chown root:guest /home/guest/simpleid2, chmod u+s
/home/guest/simpleid2 (рис.Nº3)



```
guest@localhost:/home/guest
[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Desktop
drwx----- 2 guest guest  19 Sep 26 14:49 dir1
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest  53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwxrwxr-x. 1 root  guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r--. 1 guest guest  304 Oct 3 16:24 simpleid2.c
-rw-rw-r--. 1 guest guest  175 Oct 3 16:11 simpleid.c
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Templates
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Videos
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Desktop
drwx----- 2 guest guest  19 Sep 26 14:49 dir1
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest  53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest   6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwsrwxr-x. 1 root  guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r--. 1 guest guest  304 Oct 3 16:24 simpleid2.c
-rw-rw-r--. 1 guest guest  175 Oct 3 16:11 simpleid.c
```

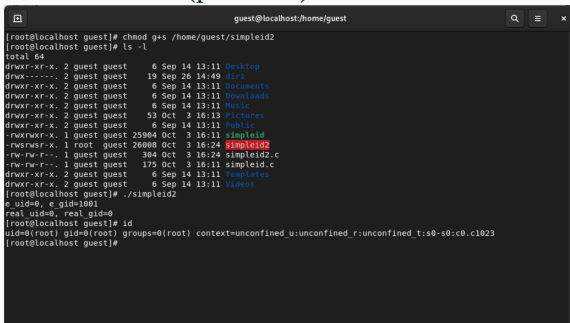
Изменение права readfile

4. Сменил владельца у файла readfile.c на vnikikita и изменил права так, чтобы только суперпользователь мог прочитать его, а guest не мог.(рис.Nº4)



```
guest@localhost:/home/guest
[root@localhost guest]# chown vnikikita readfile.c
[root@localhost guest]# ls -l readfile.c
-rw-rw-r--. 1 vnikikita guest 403 Oct 3 16:40 readfile.c
[root@localhost guest]# chmod ugo-r readfile.c
[root@localhost guest]# ls -l readfile.c
--w--w--w. 1 vnikikita guest 403 Oct 3 16:40 readfile.c
[root@localhost guest]# cat 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@localhost guest]#
```

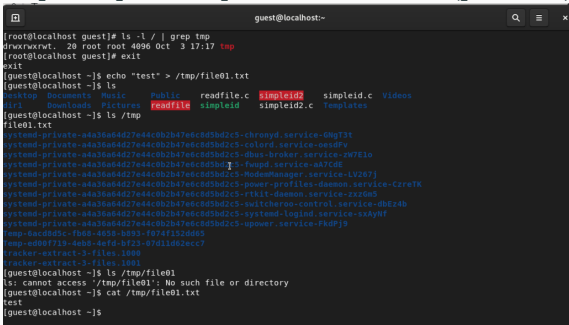
5. Прodelал теже самые пункты с SETUID относительно SetGID-бита. (рис.№5)



```
guest@localhost:/home/guest
[root@localhost guest]# chmod g+s /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Desktop
drwx----- 2 guest guest 19 Sep 26 14:49 dir1
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest 53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwsrwsr-x. 1 root  guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r-- 1 guest guest  304 Oct 3 16:24 simpleid2.c
-rw-rw-r-- 1 guest guest  175 Oct 3 16:11 simpleid.c
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Templates
drwxr-xr-x. 2 guest guest  6 Sep 14 13:11 Videos
[root@localhost guest]# ./simpleid2
e uid=0, e gid=1001
real uid=0, real gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023
[root@localhost guest]#
```


Создание файла file01 в директории tmp

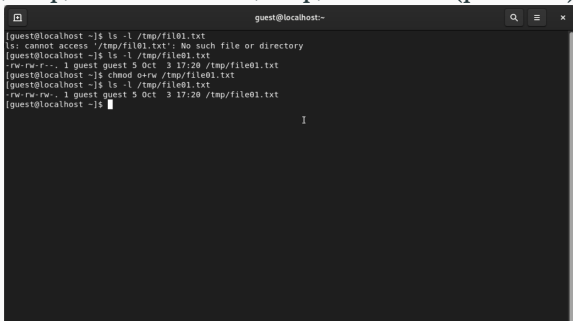
6. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test: (рис.Nº6)



```
guest@localhost:~  
[root@localhost guest]# ls -l / | grep tmp  
drwxrwxrwt. 20 root root 4096 Oct 3 17:17 tmp  
[root@localhost guest]# exit  
exit  
[guest@localhost ~]$ echo "test" > /tmp/file01.txt  
[guest@localhost ~]$ ls  
Desktop Documents Music Public readfile.c simpleid.c simpleid2.c Templates Videos  
dir1 Downloads Pictures readfile simpleid simpleid2.c Templates  
[guest@localhost ~]$ ls /tmp  
file01.txt  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-chrond.service-0NgT3t  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-colord.service-oesdFv  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-dbus-broker.service-zw7E1o  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-fuppd.service-aA7C0E  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-ModemManager.service-LV267j  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-power-profiles-daemon.service-CzreTK  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-rtkit-daemon.service-zxz6m5  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-switcheroo-control.service-dBEz4b  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-systemd-logind.service-xxAynF  
systemd-private-a4a36a8d27e44c0b2b47e6c8d5bd2c5-upower.service-FkDPj9  
femp-6acd8d5c-fb68-4658-b993-f074f132dd65  
femp-ad8b7f19-d688-34fd-b723-07d1a02ecc7  
tracker-extract-3-files-1000  
tracker-extract-3-files-1001  
[guest@localhost ~]$ ls /tmp/file01  
ls: cannot access '/tmp/file01': No such file or directory  
[guest@localhost ~]$ cat /tmp/file01.txt  
test  
[guest@localhost ~]$
```

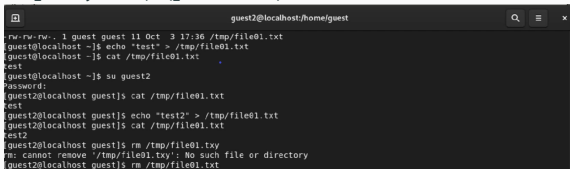
Изменение прав доступа file01

7. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: `ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt` (рис.Nº7)



```
guest@localhost:~  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
ls: cannot access '/tmp/file01.txt': No such file or directory  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 Oct 3 17:20 /tmp/file01.txt  
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 Oct 3 17:20 /tmp/file01.txt  
[guest@localhost ~]$
```

8. Повторил предыдущие шаги без без sticky-бита(без атрибута t) (рис.Nº8)



```
guest2@localhost/home/guest
-rw-rw-rw-. 1 guest guest 11 Oct  3 17:36 /tmp/file01.txt
guest@localhost ~]$ echo "test" > /tmp/file01.txt
guest@localhost ~]$ cat /tmp/file01.txt
test
guest@localhost ~]$ su guest2
Password:
guest2@localhost guest]$ cat /tmp/file01.txt
test
guest2@localhost guest]$ echo "test2" > /tmp/file01.txt
guest2@localhost guest]$ cat /tmp/file01.txt
test2
guest2@localhost guest]$ rm /tmp/file01.txy
rm: cannot remove '/tmp/file01.txy': No such file or directory
guest2@localhost guest]$ rm /tmp/file01.txt
```

Получил практические навыки работы в консоли с расширенными атрибутами файлов.