

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

Дисциплина: Основы информационной безопасности

---

Ганина Т. С.

12 апреля 2024

Группа НКАбд-01-22

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Ганина Таисия
- Студентка 2 курса, НКАбд-01-22
- Направление “Компьютерные и информационные науки”
- Российский университет дружбы народов
- Гитхаб
- <https://tsganina.github.io/>

## Вводная часть

---

- Работа с атрибутами файлов

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

---

```
[guest@tsganina ~]$ su
Пароль:
[root@tsganina guest]# setenforce 0
[root@tsganina guest]# getenforce
Permissive
[root@tsganina guest]#
```



```
guest@tsganina:/home/guest — gedit simpleid.c
r/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/
--enable-shared --enable-threads=posix --enable-checking=release --with-system-
zlib --enable-__cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-ob
ject --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --en
able-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu
--enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect
-function --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_
32=x86-64 --build=x86_64-redhat-linux --
-link-serialization=1
Модель многопоточности: posix
Supported LTO compression algorithms: zl
gcc версия 11.4.1 20230605 (Red Hat 11.4
[guest@tsganina ~]$ setenforce 0
setenforce: security_setenforce() faile
[guest@tsganina ~]$ su
Пароль:
[root@tsganina guest]# setenforce 0
[root@tsganina guest]# getenforce
Permissive
[root@tsganina guest]# touch simpleid.c
[root@tsganina guest]# gedit simpleid.c

(gedit:92280): dconf-WARNING **: 14:01:2
: Ошибка при получении данных: Соединени
```

```
Открыть ▾
simp
/home

1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4 int
5 main ()
6 {
7     uid_t uid = geteuid ();
8     gid_t gid = getegid ();
9     printf ("uid=%d, gid=%d\n", uid, gid);
10    return 0;
11 }
```

```
[root@tsganina guest]# gcc simpleid.c -o simpleid
[root@tsganina guest]# ./simpleid
uid=0, gid=0
[root@tsganina guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
[root@tsganina guest]#
```

Открыть ▼



simpleid2.c

/home/guest

```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4 int
5 main ()
6 {
7     uid_t real_uid = getuid ();
8     uid_t e_uid = geteuid ();
9     gid_t real_gid = getgid ();
10    gid_t e_gid = getegid () ;
11    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
12    printf ("real_uid=%d, real_gid=%d\n", real_uid,
13           real_gid);
14    return 0;
15 }
```

```
guest@tsganina:/home/guest

: Ошибка при получении данных: Соединение разорвано другой стороной

** (gedit:92434): WARNING **: 14:06:02.587: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается

** (gedit:92434): WARNING **: 14:06:02.587: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается

** (gedit:92434): WARNING **: 14:06:03.556: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается

** (gedit:92434): WARNING **: 14:06:03.557: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается

** (gedit:92434): WARNING **: 14:06:17.370: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается

(gedit:92434): dconf-WARNING **: 14:06:17.400: failed to commit changes to dconf
: Ошибка при получении данных: Соединение разорвано другой стороной
[root@tsganina guest]# gcc simpleid2.c -o simpleid2
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@tsganina guest]#
```

```
guest@tsganina:/home/guest

** (gedit:92434): WARNING **: 14:06:17.370: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается

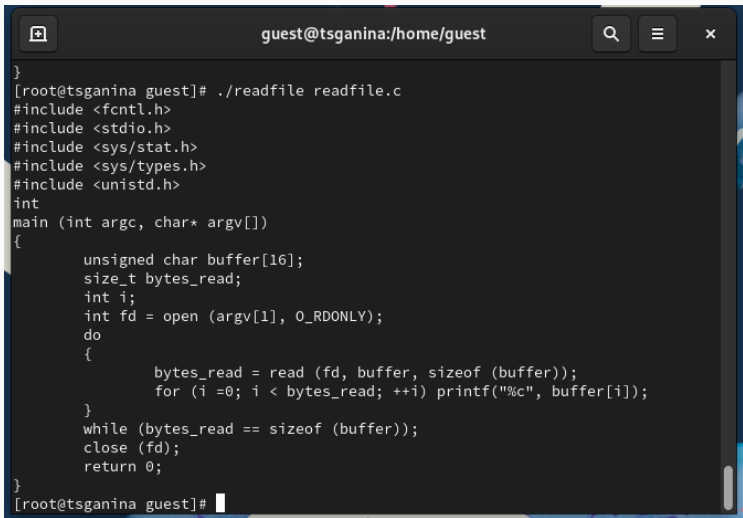
(gedit:92434): dconf-WARNING **: 14:06:17.400: failed to commit changes to dconf: Ошибка при получении данных: Соединение разорвано другой стороной
[root@tsganina guest]# gcc simpleid2.c -o simpleid2
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@tsganina guest]# chown root:guest /home/guest/simpleid2
[root@tsganina guest]# chmod u+s /home/guest/simpleid2
[root@tsganina guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 anp 12 14:06 simpleid2
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@tsganina guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tsganina guest]# chown root:guest simpleid2
[root@tsganina guest]# chmod g+s simpleid2
[root@tsganina guest]# ls -l simpleid2
-rwxr-sr-x. 1 root guest 26064 anp 12 14:06 simpleid2
[root@tsganina guest]#
```

```
guest@tsganina:/home/guest
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@tsganina guest]# chown root:guest /home/guest/simpleid2
[root@tsganina guest]# chmod u+s /home/guest/simpleid2
[root@tsganina guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 anp 12 14:06 simpleid2
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@tsganina guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tsganina guest]# chown root:guest simpleid2
[root@tsganina guest]# chmod g+s simpleid2
[root@tsganina guest]# ls -l simpleid2
-rwxr-sr-x. 1 root guest 26064 anp 12 14:06 simpleid2
[root@tsganina guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@tsganina guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tsganina guest]#
```

```
[root@tsganina guest]# gcc readfile.c -o readfile
[root@tsganina guest]# chown root:guest readfile
[root@tsganina guest]# chmod 700 readfile
[root@tsganina guest]# chown root:guest readfile
[root@tsganina guest]# chmod -r readfile.c
[root@tsganina guest]# chmod u+s readfile
[root@tsganina guest]# exit
exit
[guest@tsganina ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@tsganina ~]$
```

```
[root@tsganina guest]# exit
exit
[guest@tsganina ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@tsganina ~]$ ./readfile readfile.c
bash: ./readfile: Отказано в доступе
[guest@tsganina ~]$ ./readfile /etc/shadow
bash: ./readfile: Отказано в доступе
[guest@tsganina ~]$
```





```
guest@tsganina:/home/guest
}
[root@tsganina guest]# ./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;
}
[root@tsganina guest]#
```

```
[guest@tsganina ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 anp 12 14:33 tmp
[guest@tsganina ~]$ echo "test" > /tmp/file01.txt
[guest@tsganina ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 anp 12 14:35 /tmp/file01.txt
[guest@tsganina ~]$ chmod o+rw /tmp/file01.txt
[guest@tsganina ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 anp 12 14:35 /tmp/file01.txt
[guest@tsganina ~]$
```

```
FW 1 FW 1 guest-guest-3 tmp 12 14:55 /tmp/file01.txt
[guest@tsganina ~]$ su guest2
Пароль:
[guest2@tsganina guest]$ cat /tmp/file01.txt
test
[guest2@tsganina guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Нет такого файла или каталога
[guest2@tsganina guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$
```

```
bash: /tmp/file01.txt: нет такого файла или каталога
[guest2@tsganina guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$
```

```
[guest2@tsganina guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$ cat /tmp/file01.txt
test
[guest2@tsganina guest]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@tsganina guest]$
```

```
[guest2@tsganina guest]$ su -  
Пароль:  
[root@tsganina ~]# chmod -t /tmp  
[root@tsganina ~]# exit  
выход  
[guest2@tsganina guest]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 апр 12 14:42 tmp  
[guest2@tsganina guest]$
```

```
[guest2@tsganina guest]$ cat /tmp/file01.txt
test
[guest2@tsganina guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@tsganina guest]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
```

```
[guest2@tsganina guest]$ ls /tmp
HcRfYpzV4M
systemd-private-1d31b221501f43f98e958d52ecc570d0-chrond.service-BHxbxq
systemd-private-1d31b221501f43f98e958d52ecc570d0-colord.service-xPkNig
systemd-private-1d31b221501f43f98e958d52ecc570d0-dbus-broker.service-lL4Ry4
systemd-private-1d31b221501f43f98e958d52ecc570d0-fwupd.service-01TZE5
systemd-private-1d31b221501f43f98e958d52ecc570d0-ModemManager.service-vkWlX
systemd-private-1d31b221501f43f98e958d52ecc570d0-power-profiles-daemon.service-B
3mCws
systemd-private-1d31b221501f43f98e958d52ecc570d0-rtkit-daemon.service-w12cBn
systemd-private-1d31b221501f43f98e958d52ecc570d0-switcheroo-control.service-6opq
QN
systemd-private-1d31b221501f43f98e958d52ecc570d0-systemd-logind.service-oT0cqP
systemd-private-1d31b221501f43f98e958d52ecc570d0-upower.service-wqabHK
Temp-432273a9-39df-45ee-aafa-7401bee62e20
tmpaddon
tmpaddon-1
tmpaddon-2
vboxguest-Module.symvers
[guest2@tsganina guest]$
```



```
vboxguest module.symbols  
[guest2@tsganina guest]$ su -  
Пароль:  
[root@tsganina ~]# chmod +t /tmp  
[root@tsganina ~]# exit  
выход  
[guest2@tsganina guest]$
```

## Результаты

---

Были изучены механизмы изменения идентификаторов и применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Были рассмотрены работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов