

# Лабораторная работа №4

Основы информационной безопасности

---

Астраханцева А. А.

13 апреля 2024

Российский университет дружбы народов, Москва, Россия

- Астраханцева Анастасия Александровна
- студентка НКАбд-01-22
- Студ. билет: 1132226437
- Российский университет дружбы народов
- <https://anastasiia7205.github.io/>



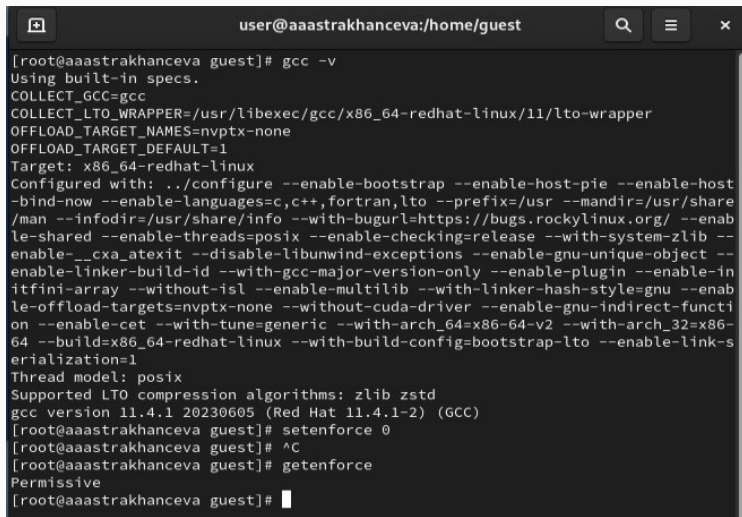
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов.

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

---



```
user@aaastrakhanceva:/home/guest

[root@aaastrakhanceva guest]# gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Target: x86_64-redhat-linux
Configured with: ../configure --enable-bootstrap --enable-host-pie --enable-host
-bind-now --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share
/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enab
le-shared --enable-threads=posix --enable-checking=release --with-system-zlib --
enable-__cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --
enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-in
itfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enab
le-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-functi
on --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_32=x86-
64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-s
erialization=1
Thread model: posix
Supported LTO compression algorithms: zlib zstd
gcc version 11.4.1 20230605 (Red Hat 11.4.1-2) (GCC)
[root@aaastrakhanceva guest]# setenforce 0
[root@aaastrakhanceva guest]# ^C
[root@aaastrakhanceva guest]# getenforce
Permissive
[root@aaastrakhanceva guest]#
```

Рис. 1: Подготовка лабораторного стенда

## Создание программы simpleid.c



The image shows a terminal window and a code editor. The terminal window at the top displays the commands `touch simpleid.c` and `gedit simpleid.c` being executed in a shell. Below the terminal, the gedit code editor is open, showing the contents of `*simpleid.c`. The code is a C program that includes `<sys/types.h>`, `<unistd.h>`, and `<stdio.h>`. It defines an `int` type and a `main` function. Inside `main`, it calls `geteuid()` and `getegid()` to retrieve the effective user and group IDs, and then prints them using `printf`. The program ends with `return 0;`.

```
guest@aaastrakhanceva:~ — gedit simpleid.c

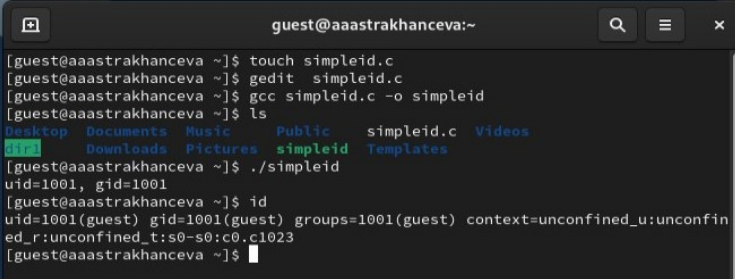
[guest@aaastrakhanceva ~]$ touch simpleid.c
[guest@aaastrakhanceva ~]$ gedit simpleid.c

Open ▾ *simpleid.c
~/

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 }
```

Рис. 2: Создание программы simpleid.c

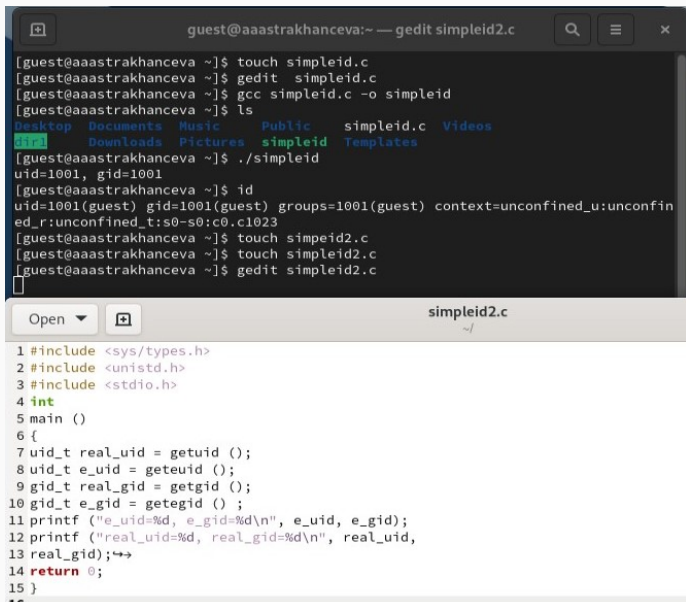
## Компиляция программы simpleid.c



```
guest@aaastrakhanceva:~  
[guest@aaastrakhanceva ~]$ touch simpleid.c  
[guest@aaastrakhanceva ~]$ gedit simpleid.c  
[guest@aaastrakhanceva ~]$ gcc simpleid.c -o simpleid  
[guest@aaastrakhanceva ~]$ ls  
Desktop  Documents  Music      Public      simpleid.c  Videos  
dir1     Downloads  Pictures   simpleid    Templates  
[guest@aaastrakhanceva ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@aaastrakhanceva ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@aaastrakhanceva ~]$
```

Рис. 3: Компиляция и запуск программы simpleid.c

## Создание программы simpleid2.c



The image shows a terminal window and a code editor. The terminal window, titled "guest@aaastrakhanceva:~ — gedit simpleid2.c", displays the following commands and output:

```
[guest@aaastrakhanceva ~]$ touch simpleid.c
[guest@aaastrakhanceva ~]$ gedit simpleid.c
[guest@aaastrakhanceva ~]$ gcc simpleid.c -o simpleid
[guest@aaastrakhanceva ~]$ ls
Desktop  Documents  Music      Public      simpleid.c  Videos
Downloads  Pictures  simpleid  Templates
[guest@aaastrakhanceva ~]$ ./simpleid
uid=1001, gid=1001
[guest@aaastrakhanceva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@aaastrakhanceva ~]$ touch simpleid2.c
[guest@aaastrakhanceva ~]$ touch simpleid2.c
[guest@aaastrakhanceva ~]$ gedit simpleid2.c
```

The code editor, titled "simpleid2.c", shows the following C code:

```
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 }
16
```

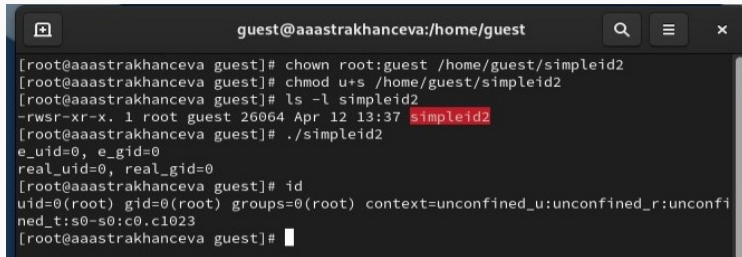


## Компиляция программы simpleid2.c

```
[guest@aaastrakhanceva ~]$ gcc simpleid2.c -o simpleid2
simpleid2.c: In function 'main':
simpleid2.c:13:11: error: stray '\342' in program
   13 | real_gid);↵
       |           ^
simpleid2.c:13:12: error: stray '\342' in program
   13 | real_gid);↵
       |           ^
[guest@aaastrakhanceva ~]$ gedit simpleid2.c
[guest@aaastrakhanceva ~]$ gcc simpleid2.c -o simpleid2
[guest@aaastrakhanceva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@aaastrakhanceva ~]$
```

Рис. 5: Компиляция программы simpleid2.c

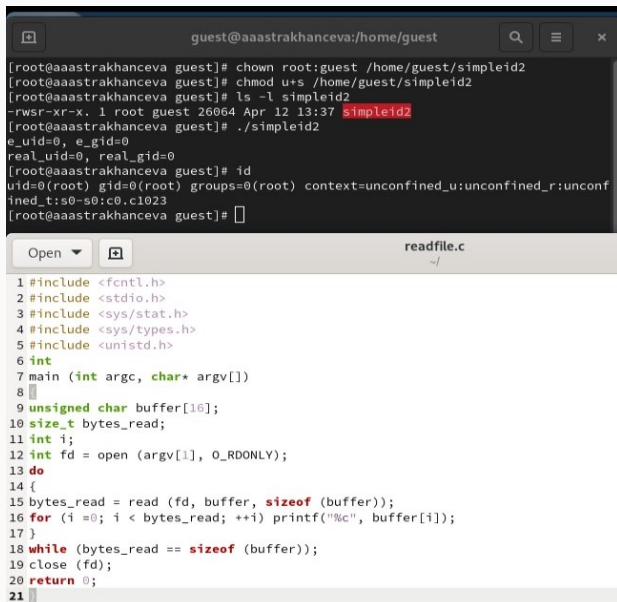
## Запуск программы simpleid2.c



```
guest@aaastrakhanceva:/home/guest
[root@aaastrakhanceva guest]# chown root:guest /home/guest/simpleid2
[root@aaastrakhanceva guest]# chmod u+s /home/guest/simpleid2
[root@aaastrakhanceva guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Apr 12 13:37 simpleid2
[root@aaastrakhanceva guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@aaastrakhanceva guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[root@aaastrakhanceva guest]#
```

Рис. 6: Изменение владельца и прав доступа для simpleid2

## Создание программы readfile.c



The image shows a terminal window and a code editor. The terminal window, titled 'guest@aaastrakhanceva:/home/guest', displays the following commands and output:

```
[root@aaastrakhanceva guest]# chown root:guest /home/guest/simpleid2
[root@aaastrakhanceva guest]# chmod u+s /home/guest/simpleid2
[root@aaastrakhanceva guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Apr 12 13:37 simpleid2
[root@aaastrakhanceva guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@aaastrakhanceva guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@aaastrakhanceva guest]#
```

The code editor, titled 'readfile.c', shows the following C code:

```
1 #include <fcntl.h>
2 #include <stdio.h>
3 #include <sys/stat.h>
4 #include <sys/types.h>
5 #include <unistd.h>
6 int
7 main (int argc, char* argv[])
8 {
9     unsigned char buffer[16];
10    size_t bytes_read;
11    int i;
12    int fd = open (argv[1], O_RDONLY);
13    do
14    {
15        bytes_read = read (fd, buffer, sizeof (buffer));
16        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
17    }
18    while (bytes_read == sizeof (buffer));
19    close (fd);
20    return 0;
21 }
```

## Компиляция и запуск программы readfile.c

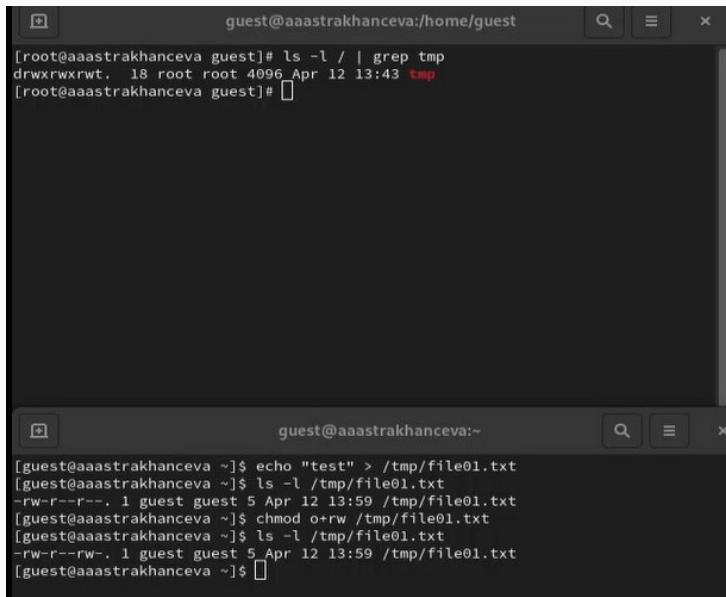
```
guest@aaastrakhanceva:/home/guest

[root@aaastrakhanceva guest]# chown root:guest readfile
[root@aaastrakhanceva guest]# chmod 700 readfile
[root@aaastrakhanceva guest]# chown root:guest readfile
[root@aaastrakhanceva guest]# chmod -r readfile
[root@aaastrakhanceva guest]# cchmod u+s readfile
bash: cchmod: command not found...
[root@aaastrakhanceva guest]# chmod u+s readfile
[root@aaastrakhanceva guest]#

guest@aaastrakhanceva:~

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@aaastrakhanceva ~]$ cat readfile
cat: readfile: Permission denied
[guest@aaastrakhanceva ~]$ ./readfile readfile.c
bash: ./readfile: Permission denied
[guest@aaastrakhanceva ~]$ cat readfile
cat: readfile: Permission denied
[guest@aaastrakhanceva ~]$ ./readfile readfile.c
bash: ./readfile: Permission denied
[guest@aaastrakhanceva ~]$ ./readfile /etc/shadow
bash: ./readfile: Permission denied
[guest@aaastrakhanceva ~]$
```

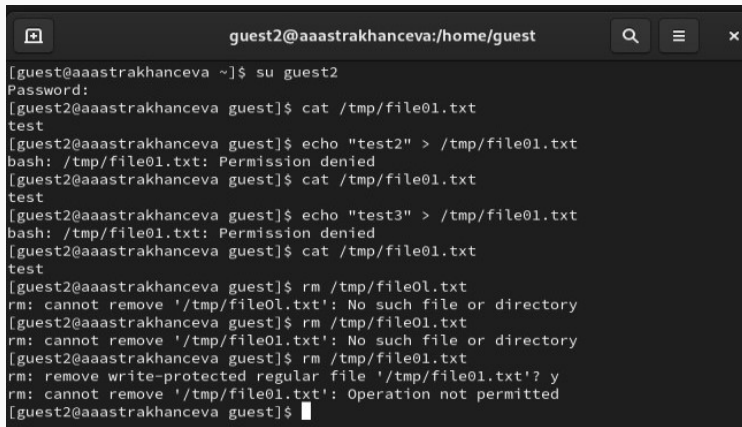
## Исследование Sticky-бита



The image shows two terminal windows. The top window is titled 'guest@aaastrakhanceva:/home/guest' and shows a command 'ls -l / | grep tmp' being executed. The output is 'drwxrwxrwt. 18 root root 4096 Apr 12 13:43 tmp'. The bottom window is titled 'guest@aaastrakhanceva:~' and shows a sequence of commands: 'echo "test" > /tmp/file01.txt', 'ls -l /tmp/file01.txt', 'chmod o+rw /tmp/file01.txt', and another 'ls -l /tmp/file01.txt'. The output of the second 'ls' command shows the file permissions as '-rw-r--rw-. 1 guest guest 5 Apr 12 13:59 /tmp/file01.txt'.

```
guest@aaastrakhanceva:/home/guest
[root@aaastrakhanceva guest]# ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Apr 12 13:43 tmp
[root@aaastrakhanceva guest]#

guest@aaastrakhanceva:~
[guest@aaastrakhanceva ~]$ echo "test" > /tmp/file01.txt
[guest@aaastrakhanceva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Apr 12 13:59 /tmp/file01.txt
[guest@aaastrakhanceva ~]$ chmod o+rw /tmp/file01.txt
[guest@aaastrakhanceva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Apr 12 13:59 /tmp/file01.txt
[guest@aaastrakhanceva ~]$
```



```
guest2@aaastrakhanceva:/home/guest

[guest@aaastrakhanceva ~]$ su guest2
Password:
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@aaastrakhanceva guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@aaastrakhanceva 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@aaastrakhanceva guest]$
```

Рис. 10: От лица guest2 попытка прочесть файл, изменить его и удалить его

```
[guest2@aaastrakhanceva guest]$ su -  
Password:  
[root@aaastrakhanceva ~]# chmod -t /tmp  
[root@aaastrakhanceva ~]# exit  
logout  
[guest2@aaastrakhanceva guest]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 Apr 12 14:08 tmp
```

Рис. 11: Переход в режим суперпользователя, снятие Sticky бита

```
[guest2@aaastrakhanceva guest]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 Apr 12 14:08 tmp
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aaastrakhanceva guest]$ cat /tmp/file01.txt
test
[guest2@aaastrakhanceva guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@aaastrakhanceva guest]$ ls /tmp
systemd-private-bd9ab20792b04d54ae93f80037242902-chrond.service-fDRJsn
systemd-private-bd9ab20792b04d54ae93f80037242902-colord.service-CkEISg
systemd-private-bd9ab20792b04d54ae93f80037242902-dbus-broker.service-WzEajM
systemd-private-bd9ab20792b04d54ae93f80037242902-fwupd.service-DIqn3I
systemd-private-bd9ab20792b04d54ae93f80037242902-kdump.service-AmdVHn
systemd-private-bd9ab20792b04d54ae93f80037242902-ModemManager.service-8Pjibz
systemd-private-bd9ab20792b04d54ae93f80037242902-power-profiles-daemon.service-Bt5C3Z
systemd-private-bd9ab20792b04d54ae93f80037242902-rtkit-daemon.service-yWzqqS
systemd-private-bd9ab20792b04d54ae93f80037242902-switcheroo-control.service-GrhEGF
systemd-private-bd9ab20792b04d54ae93f80037242902-systemd-logind.service-KimgXH
systemd-private-bd9ab20792b04d54ae93f80037242902-upower.service-YXTirc
tmp-f57bb7af-56b2-4ef1-8ce4-50bfb4fc10e1
[guest2@aaastrakhanceva guest]$ cd /tmp | grep file01.txt
```

Рис. 12: Повторение пунктов 4-9 со снятым Sticky битом



В ходе выполнения лабораторной работы я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Также 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.

Спасибо за внимание

---