

# Презентация по по лабораторной работе №5

Основы информационной безопасности

---

Паращенко А.Д.

1 октября 2024

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

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

Получение практических навыков работы в консоли с дополнительными атрибутами.

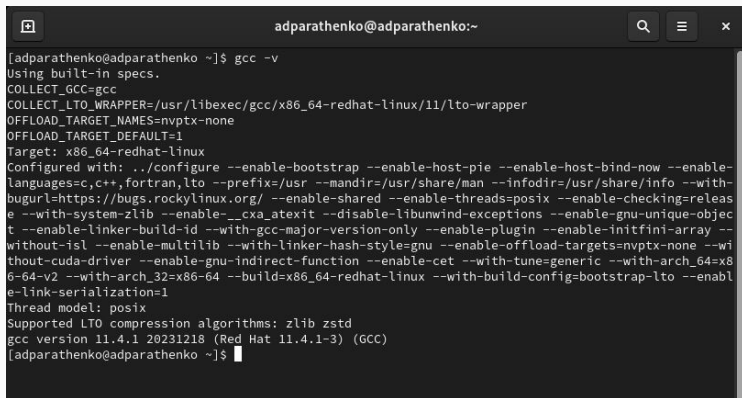
Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Выполнение лабораторной работы

---

# Подготовка к выполнению лабораторной работы

1) Проверяем установлен ли компилятор gcc командой `gcc -v` (рис. (fig:001?))



```
adparathenko@adparathenko:~  
[adparathenko@adparathenko ~]$ 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/ --enable-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-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 --with-build-config=bootstrap-lto --enable-link-serialization=1  
Thread model: posix  
Supported LTO compression algorithms: zlib zstd  
gcc version 11.4.1 20231218 (Red Hat 11.4.1-3) (GCC)  
[adparathenko@adparathenko ~]$
```

Рис. 1: gcc -v

Создание программы

- 1) Войдите в систему от имени пользователя guest.
- 2) Создайте программу simpleid.c (рис. (fig:004?)) - (рис. (fig:005?))

```
compilation terminated.
[quest@adparathenko ~]$ touch simpleid.c
[quest@adparathenko ~]$ ls
Desktop  dir1  dir2  Documents  Downloads  Music  Pictures  Public  simpleid.c  Templates  Videos
[quest@adparathenko ~]$ gedit simpleid.c

(gedit:7194): dbind-WARNING **: 20:38:21.462: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

(gedit:7194): dconf-WARNING **: 20:38:21.800: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:21.808: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:7194): WARNING **: 20:41:44.630: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7194): WARNING **: 20:41:44.631: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:7194): WARNING **: 20:41:46.215: Set document metadata failed: Setting attribute metadata
```

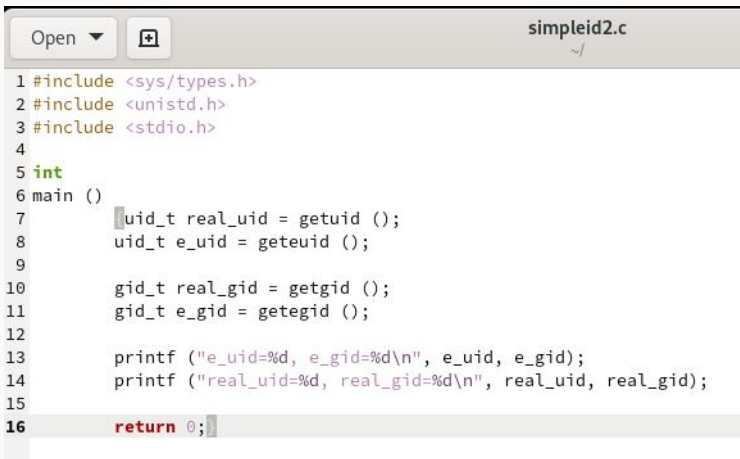
- 3) Скомпилировали программу и убедились, что файл программы создан *gcc simpleid.c -o simpleid*
- 4) Выполняем программу simpleid
- 5) Выполняем системную программу id и сравниваем результаты.(рис. (fig:006?))

```
[quest@adparathenko ~]$ gcc simpleid.c -o simpleid
[quest@adparathenko ~]$ ./simpleid
uid=1001, gid=1001
[quest@adparathenko ~]$ id
uid=1001(quest) gid=1001(quest) groups=1001(quest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[quest@adparathenko ~]$
```

Рис. 6: Выполнение программы simpleid.c и id



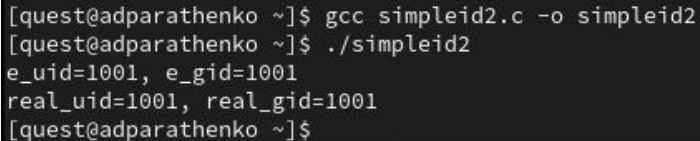
- 6) Усложняем программу, добавив вывод действительных идентификаторов.  
Получившуюся программу назовите simpleid2.c. (рис. (fig:007?))



```
simpleid2.c
~/

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

- 7) Компилируем и запускаем simpleid2.c: `gcc simpleid2.c -o simpleid2 ./simpleid2` (рис. (fig:008?))



```
[quest@adparathenko ~]$ gcc simpleid2.c -o simpleid2
[quest@adparathenko ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[quest@adparathenko ~]$
```

Рис. 8: Запуск программы simpleid2.c

- 8) От имени суперпользователя выполните команды: *chown root:quest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2*
- 9) Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2: *ls -l simpleid2* (рис. (fig:009?))

```
[adparathenko@adparathenko ~]$ sudo chown root:quest /home/guest/simpleid2
[adparathenko@adparathenko ~]$ sudo chmod u+s /home/guest/simpleid2
[adparathenko@adparathenko ~]$ sudo ls -l /home/guest/simpleid2
ls: cannot access '-': No such file or directory
ls: cannot access 'l': No such file or directory
/home/guest/simpleid2
[adparathenko@adparathenko ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root quest 24488 Sep 30 20:50 /home/guest/simpleid2
[adparathenko@adparathenko ~]$
```

Рис. 9: Установка атрибутов

11) Запускаем simpleid2 и id: *./simpleid2 id* и сравниваем результаты. (рис. (fig:010?))

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

Рис. 10: Программа simpleid2.c и id

### 13) Создайте программу readfile.c: (рис. (fig:011?)) - (рис. (fig:012?))

```

[quest@adparathenko ~]$ touch readfile.c
[quest@adparathenko ~]$ gedit readfile.c

(gedit:7622): dbind-WARNING **: 21:00:02.494: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

(gedit:7622): dconf-WARNING **: 21:00:02.591: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.600: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.844: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.845: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.849: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

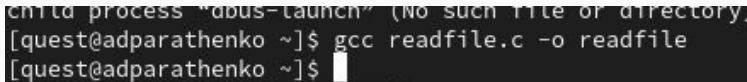
** (gedit:7622): WARNING **: 21:05:19.120: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7622): WARNING **: 21:05:19.122: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

(gedit:7622): dconf-WARNING **: 21:05:22.096: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

```

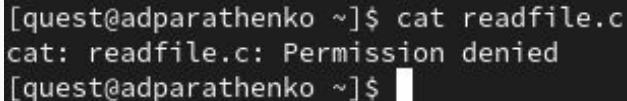
14) Откомпилируем програму readfile.c. (рис. (fig:013?))

A terminal window with a dark background and light-colored text. The text shows a previous command's output, the current user and host, and the successful execution of the gcc compiler to create an executable named 'readfile'.

```
child process "dbus-launch" (No such file or directory)  
[quest@adparathenko ~]$ gcc readfile.c -o readfile  
[quest@adparathenko ~]$
```

Рис. 13: Компилирование программы readfile.c

- 15) Меняем владельца у файла readfile.c (или любого другого текстового файла в системе) и изменяем права так, чтобы только суперпользователь(root) мог прочитать его, а guest не мог.
- 16) Проверяем, что пользователь guest не может прочитать файл readfile.c (рис. (fig:014?))

A terminal window with a black background and white text. The prompt is [quest@adparathenko ~]\$. The user enters the command cat readfile.c. The output is cat: readfile.c: Permission denied. The prompt returns to [quest@adparathenko ~]\$.

```
[quest@adparathenko ~]$ cat readfile.c
cat: readfile.c: Permission denied
[quest@adparathenko ~]$
```

Рис. 14: Чтение файла readfile.c

- 17) Меняем у программы readfile владельца и установите SetU'D-бит.
- 18) Проверяем, может ли программа readfile прочитать файл readfile.c (рис. (fig:015?))

[illegible]



19) Проверяем, может ли программа readfile прочитать файл /etc/shadow (рис. (fig:016?)) - (рис. (fig:017?))

[illegible]

## Исследование Sticky-бита

---

- 1) Выясним, установлен ли атрибут Sticky на директории /tmp командой `ls -l / | grep tmp`
- 2) От имени пользователя guest создаём файл `file01.txt` в директории /tmp со словом test:  
`echo "test" > /tmp/file01.txt`
- 3) Просмотрим атрибуты у только что созданного файла и разрешим 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. (fig:018?))

```
[quest@adparathenko ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Sep 30 21:14 tmp
[quest@adparathenko ~]$ echo "test" > /tmp/file01.txt
[quest@adparathenko ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 quest quest 5 Sep 30 21:16 /tmp/file01.txt
[quest@adparathenko ~]$ chmod 0+rw /tmp/file01.txt
chmod: invalid mode: '0+rw'
Try 'chmod --help' for more information.
[quest@adparathenko ~]$ chmod o+rw /tmp/file01.txt
[quest@adparathenko ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 quest quest 5 Sep 30 21:16 /tmp/file01.txt
```

4) От пользователя `quest2` (не являющегося владельцем) пробуем прочитать файл `/tmp/file01.txt`: `cat /tmp/file01.txt` 5) От пользователя `quest2` пробуем дозаписать в файл `/tmp/file01.txt` слово `test2` `echo "test2" > /tmp/file01.txt` 6) Проверяем содержимое файла `cat /tmp/file01.txt` 7) От пользователя `quest2` пробуем записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt` 8) Проверяем содержимое файла командой `cat /tmp/file01.txt` 9) От пользователя `quest2` пробуем удалить файл `/tmp/file01.txt` командой `rm /tmp/file01.txt` (рис. (fig:019?))

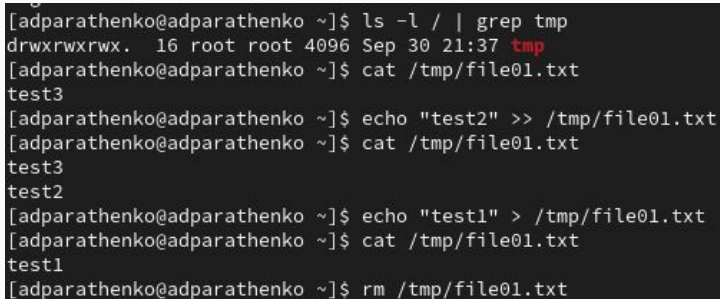
```
[quest@adparathenko ~]$ su - quest2
Password:
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test
[quest2@adparathenko ~]$ echo "test2" > /tmp/file01.txt
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test2
[quest2@adparathenko ~]$ echo "test3" > /tmp/file01.txt
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test3
[quest2@adparathenko ~]$ rm /tmp/file01.txt
```

- 10) Повышаем свои права до суперпользователя следующей командой **su -** и выполняем после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: **chmod -t /tmp**
- 11) Покидаем режим суперпользователя командой **exit** (рис. (fig:020?))

```
password etc. authentication tokens updated successfully.  
[adparathenko@adparathenko ~]$ su -  
Password:  
[root@adparathenko ~]# chmod -t /tmp  
[root@adparathenko ~]# exit  
logout  
[adparathenko@adparathenko ~]$
```

Рис. 18: Суперпользователь

- 12) От пользователя guest2 проверяем, что атрибута t у директории /tmp нет: `ls -l / | grep tmp`
- 13) Повторяем предыдущие шаги. (рис. (fig:021?))

A terminal window showing a series of commands and their outputs. The user is at the prompt [adparathenko@adparathenko ~]. The first command is 'ls -l / | grep tmp', which outputs 'drwxrwxrwx. 16 root root 4096 Sep 30 21:37 tmp'. The second command is 'cat /tmp/file01.txt', which outputs 'test3'. The third command is 'echo "test2" >> /tmp/file01.txt'. The fourth command is 'cat /tmp/file01.txt', which outputs 'test3' followed by 'test2'. The fifth command is 'echo "test1" > /tmp/file01.txt'. The sixth command is 'cat /tmp/file01.txt', which outputs 'test1'. The final command is 'rm /tmp/file01.txt'.

```
[adparathenko@adparathenko ~]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Sep 30 21:37 tmp
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test3
[adparathenko@adparathenko ~]$ echo "test2" >> /tmp/file01.txt
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test3
test2
[adparathenko@adparathenko ~]$ echo "test1" > /tmp/file01.txt
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test1
[adparathenko@adparathenko ~]$ rm /tmp/file01.txt
```

Рис. 19: Работа без атрибута t

- 15) Повышаем свои права до суперпользователя и возвращаем атрибут `t` на директорию `/tmp`: `su - chmod +t /tmp exit` (рис. (fig:022?))

```
[adparathenko@adparathenko ~]$ su -  
Password:  
[root@adparathenko ~]# chmod +t /tmp  
[root@adparathenko ~]# exit  
logout  
[adparathenko@adparathenko ~]$ ls -l / | grep tmp  
drwxrwxrwt. 16 root root 4096 Sep 30 21:45 tmp  
[adparathenko@adparathenko ~]$
```

Рис. 20: Работа без атрибута `t`

## Вывод

---



В результате выполнения работы я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Список литературы

---

- 1) [https://esystem.rudn.ru/pluginfile.php/2357153/mod\\_resource/content/2/005-lab\\_discret\\_sticky.pdf](https://esystem.rudn.ru/pluginfile.php/2357153/mod_resource/content/2/005-lab_discret_sticky.pdf)