

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Люпп Софья Романовна

Содержание

1	Цель работы.....	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы.....	2
4	Выводы.....	13
	Список литературы.....	13

1 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.

2 Теоретическое введение

1. Дополнительные атрибуты файлов Linux

В Linux существует три основных вида прав — право на чтение (read), запись (write) и выполнение (execute), а также три категории пользователей, к которым они могут применяться — владелец файла (user), группа владельца (group) и все остальные (others). Но, кроме прав чтения, выполнения и записи, есть еще три дополнительных атрибута. [1]

Sticky bit

Используется в основном для каталогов, чтобы защитить в них файлы. В такой каталог может писать любой пользователь. Но, из такой директории пользователь может удалить только те файлы, владельцем которых он является. Примером может служить директория /tmp, в которой запись открыта для всех пользователей, но нежелательно удаление чужих файлов.

SUID (Set User ID)

Атрибут исполняемого файла, позволяющий запустить его с правами владельца. В Linux приложение запускается с правами пользователя, запустившего указанное приложение. Это обеспечивает дополнительную безопасность т.к. процесс с правами пользователя

не сможет получить доступ к важным системным файлам, которые принадлежат пользователю root.

SGID (Set Group ID)

Аналогичен suid, но относиться к группе. Если установить sgid для каталога, то все файлы созданные в нем, при запуске будут принимать идентификатор группы каталога, а не группы владельца, который создал файл в этом каталоге.

Обозначение атрибутов sticky, suid, sgid

Специальные права используются довольно редко, поэтому при выводе программы ls -l символ, обозначающий указанные атрибуты, закрывает символ стандартных прав доступа.

Пример: rwsrwsrwt

где первая s — это suid, вторая s — это sgid, а последняя t — это sticky bit

В приведенном примере не понятно, rwt — это rw- или rwx? Определить это просто. Если t маленькое, значит x установлен. Если T большое, значит x не установлен. То же самое правило распространяется и на s.

В числовом эквиваленте данные атрибуты определяются первым символом при четырехзначном обозначении (который часто опускается при назначении прав), например в правах 1777 — символ 1 обозначает sticky bit. Остальные атрибуты имеют следующие числовое соответствие:

- 1 – установлен sticky bit
- 2 – установлен sgid
- 4 – установлен suid

2. Компилятор GCC

GCC - это свободно доступный оптимизирующий компилятор для языков C, C++. Собственно программа gcc это некоторая надстройка над группой компиляторов, которая способна анализировать имена файлов, передаваемые ей в качестве аргументов, и определять, какие действия необходимо выполнить. Файлы с расширением .cc или .C рассматриваются, как файлы на языке C++, файлы с расширением .c как программы на языке C, а файлы с расширением .o считаются объектными [2].

3 Выполнение лабораторной работы

Для лабораторной работы необходимо проверить, установлен ли компилятор gcc, команда gcc -v позволяет это сделать. Также осуществляется отключение системы запретом с помощью setenforce 0 (рис. 1).

```
File Actions Edit View Help
(srluipp@luipp)-[~]
$ yam install gcc
Command 'yam' not found, did you mean:
  command 'bam' from deb bam
  command 'yatm' from deb yatm
  command 'yadm' from deb yadm
  command 'nam' from deb nam
  command 'yasm' from deb yasm
  command 'vam' from deb vim-addon-manager
  command 'yad' from deb yad
  command 'cam' from deb libcamera-tools
Try: sudo apt install <deb name>

(srluipp@luipp)-[~]
$ sudo apt install gcc
[sudo] password for srluipp:
gcc is already the newest version (4:14.2.0-1).
gcc set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1546

(srluipp@luipp)-[~]
$
```

Подготовка к лабораторной работе

Осуществляется вход от имени пользователя guest (рис. 2).

```
srлуipp@луipp: ~  
File Actions Edit View Help  
Space needed: 660 kB / 18.4 GB available  
Continue? [Y/n] Y  
Get:1 http://kali.download/kali kali-rolling/main amd64 libselinux1 amd64 3.8-3 [84.6 kB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 selinux-utils amd64 3.8-3 [109 kB]  
Get:2 http://mirror.cspacehostings.com/kali kali-rolling/main amd64 libsepol2 amd64 3.8-1 [296 kB]  
Fetched 489 kB in 2s (259 kB/s)  
(Reading database ... 403786 files and directories currently installed.)  
Preparing to unpack .../libselinux1_3.8-3_amd64.deb ...  
Unpacking libselinux1:amd64 (3.8-3) over (3.7-3+b1) ...  
Setting up libselinux1:amd64 (3.8-3) ...  
/var/lib/dpkg/info/libselinux1:amd64.postinst: 6: sestatus: not found  
(Reading database ... 403785 files and directories currently installed.)  
Preparing to unpack .../libsepol2_3.8-1_amd64.deb ...  
Unpacking libsepol2:amd64 (3.8-1) over (3.7-1) ...  
Setting up libsepol2:amd64 (3.8-1) ...  
Selecting previously unselected package selinux-utils.  
(Reading database ... 403785 files and directories currently installed.)  
Preparing to unpack .../selinux-utils_3.8-3_amd64.deb ...  
Unpacking selinux-utils (3.8-3) ...  
Setting up selinux-utils (3.8-3) ...  
Processing triggers for libc-bin (2.40-3) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for kali-menu (2024.4.0) ...  
(srлуipp@луipp)-[~]  
$
```

Вход от имени пользователя guest

Создание файла simpled.c и запись в файл кода (рис. 3)

```
File Actions Edit View Help
(Reading database ... 403785 files and directories currently installed.)
Preparing to unpack .../libsepol2_3.8-1_amd64.deb ...
Unpacking libsepol2:amd64 (3.8-1) over (3.7-1) ...
Setting up libsepol2:amd64 (3.8-1) ...
Selecting previously unselected package selinux-utils.
(Reading database ... 403785 files and directories currently installed.)
Preparing to unpack .../selinux-utils_3.8-3_amd64.deb ...
Unpacking selinux-utils (3.8-3) ...
Setting up selinux-utils (3.8-3) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...

(srлуipp@луipp)-[~]
$ setenforce 0
setenforce: SELinux is disabled

(srлуipp@луipp)-[~]
$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/gcc

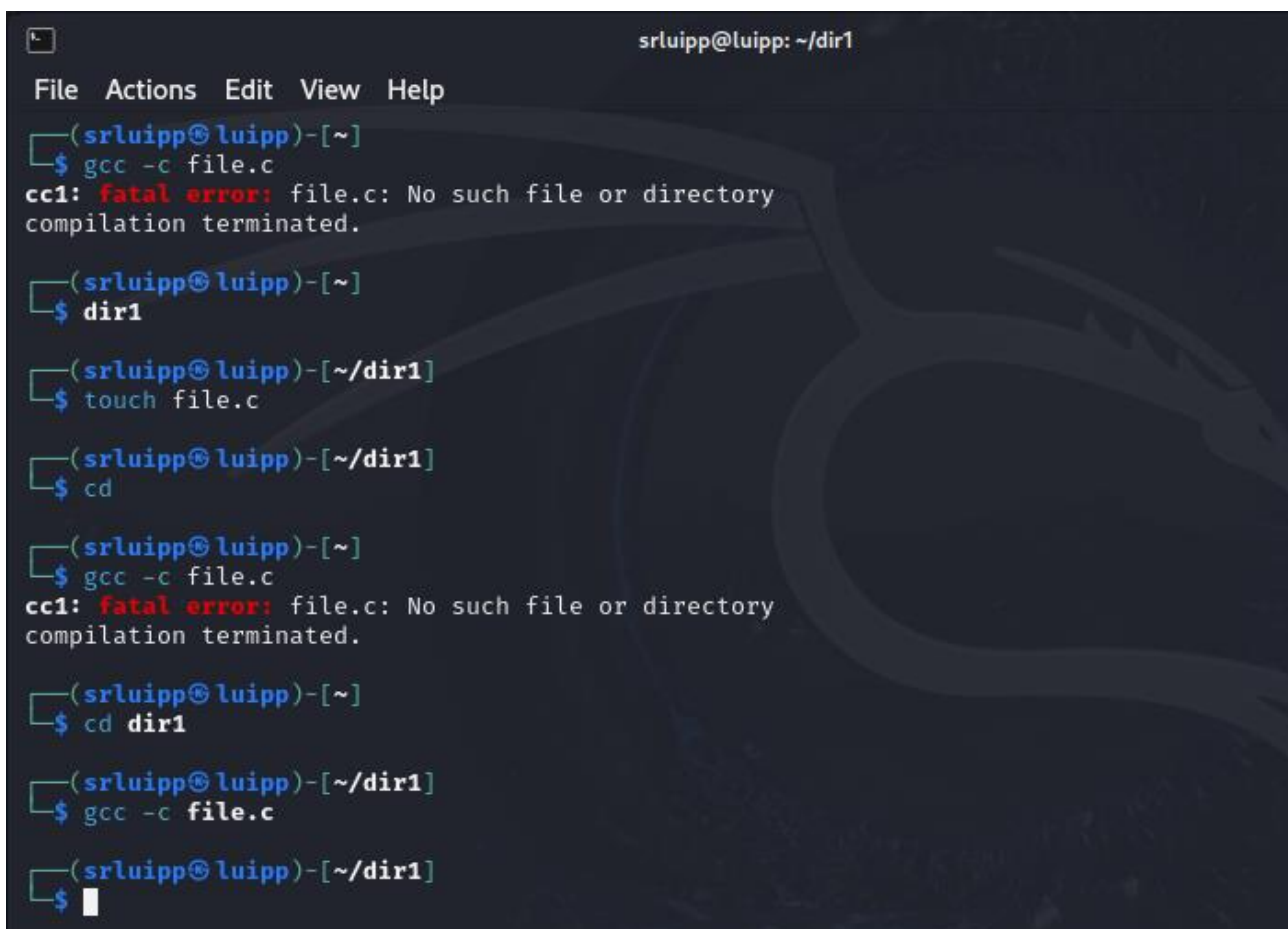
(srлуipp@луipp)-[~]
$ whereis g++
g++: /usr/bin/g++

(srлуipp@луipp)-[~]
$
```

Создание файла

С++ Листинг 1 #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; }

Содержимое файла выглядит следующим образом (рис. 4)



```
File Actions Edit View Help
(srluipp@luipp)-[~]
$ gcc -c file.c
cc1: fatal error: file.c: No such file or directory
compilation terminated.

(srluipp@luipp)-[~]
$ dir1

(srluipp@luipp)-[~/dir1]
$ touch file.c

(srluipp@luipp)-[~/dir1]
$ cd

(srluipp@luipp)-[~]
$ gcc -c file.c
cc1: fatal error: file.c: No such file or directory
compilation terminated.

(srluipp@luipp)-[~]
$ cd dir1

(srluipp@luipp)-[~/dir1]
$ gcc -c file.c

(srluipp@luipp)-[~/dir1]
$
```

Содержимое файла

Компилирую файл, проверяю, что он скомпилировался (рис. 5)

```
File Actions Edit View Help

(sruiipp@luipp)-[~/dir1]
$ touch file.c

(sruiipp@luipp)-[~/dir1]
$ cd

(sruiipp@luipp)-[~]
$ gcc -c file.c
cc1: fatal error: file.c: No such file or directory
compilation terminated.

(sruiipp@luipp)-[~]
$ cd dir1

(sruiipp@luipp)-[~/dir1]
$ gcc -c file.c

(sruiipp@luipp)-[~/dir1]
$ gcc -o program file.o
/usr/bin/ld: /usr/lib/gcc/x86_64-linux-gnu/14/../../../../x86_64-linux-gnu/Scrt1.o: in function `_start'
(.text+0x17): undefined reference to `main'
collect2: error: ld returned 1 exit status

(sruiipp@luipp)-[~/dir1]
$
```

Компиляция файла

Запускаю исполняемый файл. В выводе файла выписаны номера пользователя и групп, от вывода при вводе if, они отличаются только тем, что информации меньше (рис. 6)

```
File Actions Edit View Help

(sruiipp@luipp)-[~]
$ cd dir1

(sruiipp@luipp)-[~/dir1]
$ gcc -c file.c

(sruiipp@luipp)-[~/dir1]
$ gcc -o program file.o
day at 01:57:11 PM /usr/lib/gcc/x86_64-linux-gnu/14/../../../../x86_64-linux-gnu/Scrt1.o: in function `_start'
(.text+0x17): undefined reference to `main'
collect2: error: ld returned 1 exit status

(sruiipp@luipp)-[~/dir1]
$ ls dir1
ls: cannot access 'dir1': No such file or directory

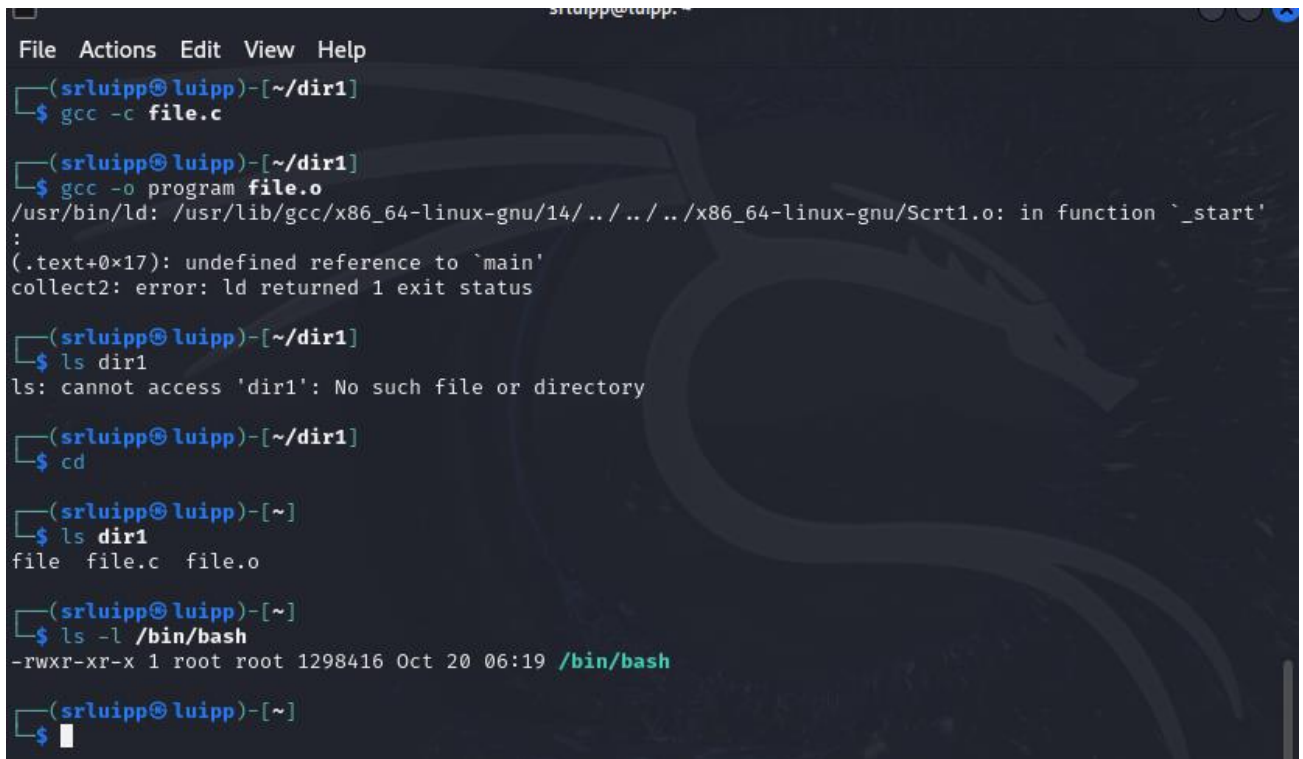
(sruiipp@luipp)-[~/dir1]
$ cd

(sruiipp@luipp)-[~]
$ ls dir1
file file.c file.o

(sruiipp@luipp)-[~]
$
```

Сравнение команд

Создание, запись в файл и компиляция файла `simplified2.c`. Запуск программы (рис. 7)



```
File Actions Edit View Help
(srLuipp@luipp)-[~/dir1]
$ gcc -c file.c

(srLuipp@luipp)-[~/dir1]
$ gcc -o program file.o
/usr/bin/ld: /usr/lib/gcc/x86_64-linux-gnu/14/../../../../x86_64-linux-gnu/Scrt1.o: in function `_start'
:
(.text+0x17): undefined reference to `main'
collect2: error: ld returned 1 exit status

(srLuipp@luipp)-[~/dir1]
$ ls dir1
ls: cannot access 'dir1': No such file or directory

(srLuipp@luipp)-[~/dir1]
$ cd

(srLuipp@luipp)-[~]
$ ls dir1
file file.c file.o

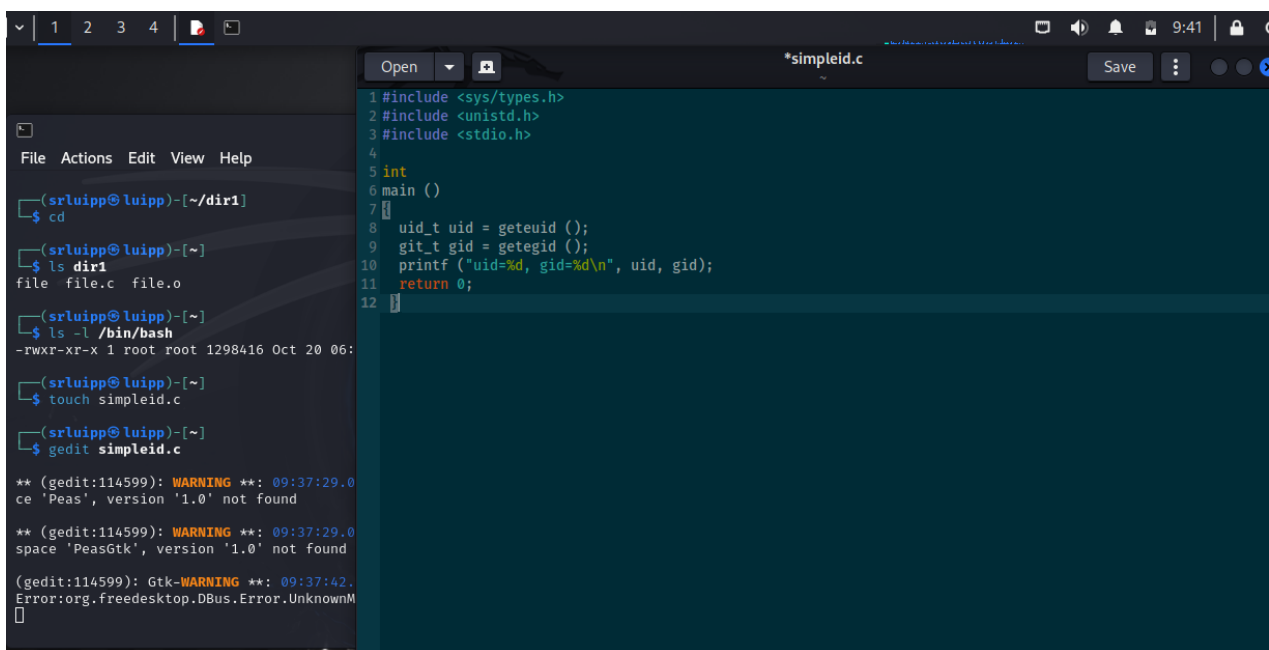
(srLuipp@luipp)-[~]
$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1298416 Oct 20 06:19 /bin/bash

(srLuipp@luipp)-[~]
$
```

Создание и компиляция файла

```
C++ Листинг 2 #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; }
```

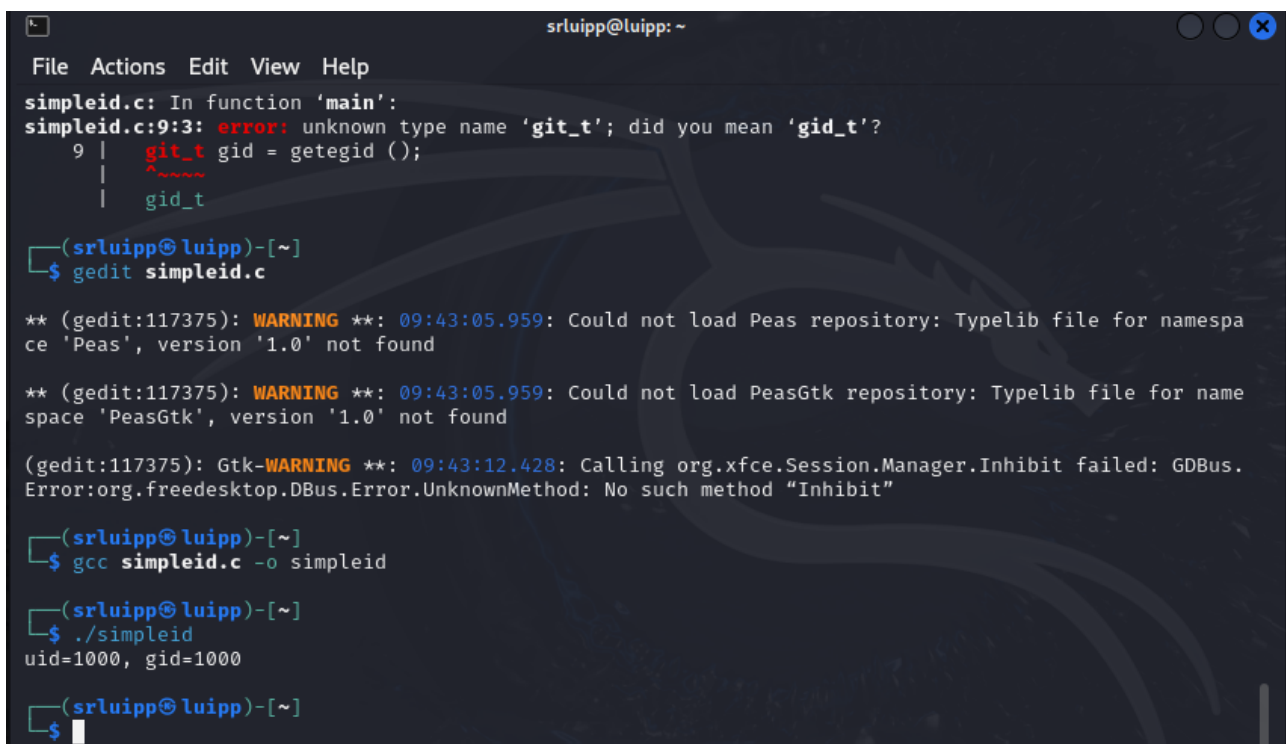
(рис. 8)



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

Содержимое файла

С помощью `chown` изменяю владельца файла на суперпользователя, с помощью `chmod` изменяю права доступа (рис. 9)



```
simpleid.c: In function 'main':
simpleid.c:9:3: error: unknown type name 'git_t'; did you mean 'gid_t'?
   9 |     git_t gid = getegid ();
     |     ~~~~~
     |     gid_t

(srluipp@luipp)-[~]
$ gcc simpleid.c -o simpleid

(srluipp@luipp)-[~]
$ ./simpleid
uid=1000, gid=1000
```

Смена владельца файла и прав доступа к файлу

Сравнение вывода программы и команды `id`, наша команда снова вывела только ограниченное количество информации (рис. 10)

```
File Actions Edit View Help
(srluipp@luipp)-[~]
$ gedit simpleid.c

** (gedit:117375): WARNING **: 09:43:05.959: Could not load Peas repository: Typelib file for namespace 'Peas', version '1.0' not found

** (gedit:117375): WARNING **: 09:43:05.959: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', version '1.0' not found

(gedit:117375): Gtk-WARNING **: 09:43:12.428: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: No such method "Inhibit"

(srluipp@luipp)-[~]
$ gcc simpleid.c -o simpleid

(srluipp@luipp)-[~]
$ ./simpleid
uid=1000, gid=1000

(srluipp@luipp)-[~]
$ id
uid=1000(srluipp) gid=1000(srluipp) groups=1000(srluipp),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),116(bluetooth),121(wireshark),123(lpadmin),129(scanner),134(vboxsf),135(kaboxer)

(srluipp@luipp)-[~]
$
```

Запуск файла

Создание и компиляция файла readfile.c (рис. 11)

```
Open *simpleid2.c Save
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t real_uid = getuid ();
9     uid_t e_uid = geteuid ();
10
11     gid_t real_gid = getgid ();
12     gid_t e_gid = getegid ();
13
14     printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
15     printf ("real_uid=%d, real_gid=%d\n", real_uid,
16           real_gid);
17
18     return 0;
19 }
```

```
File Actions Edit View Help
(srluipp@luipp)-[~]
$ touch simpleid2.c

(srluipp@luipp)-[~]
$ gedit simpleid.c

** (gedit:118560): WARNING **: 09:45:28.2 ce 'Peas', version '1.0' not found

** (gedit:118560): WARNING **: 09:45:28.2 space 'PeasGtk', version '1.0' not found

(srluipp@luipp)-[~]
$ gedit simpleid2.c

** (gedit:118661): WARNING **: 09:45:39.5 ce 'Peas', version '1.0' not found

** (gedit:118661): WARNING **: 09:45:39.5 space 'PeasGtk', version '1.0' not found

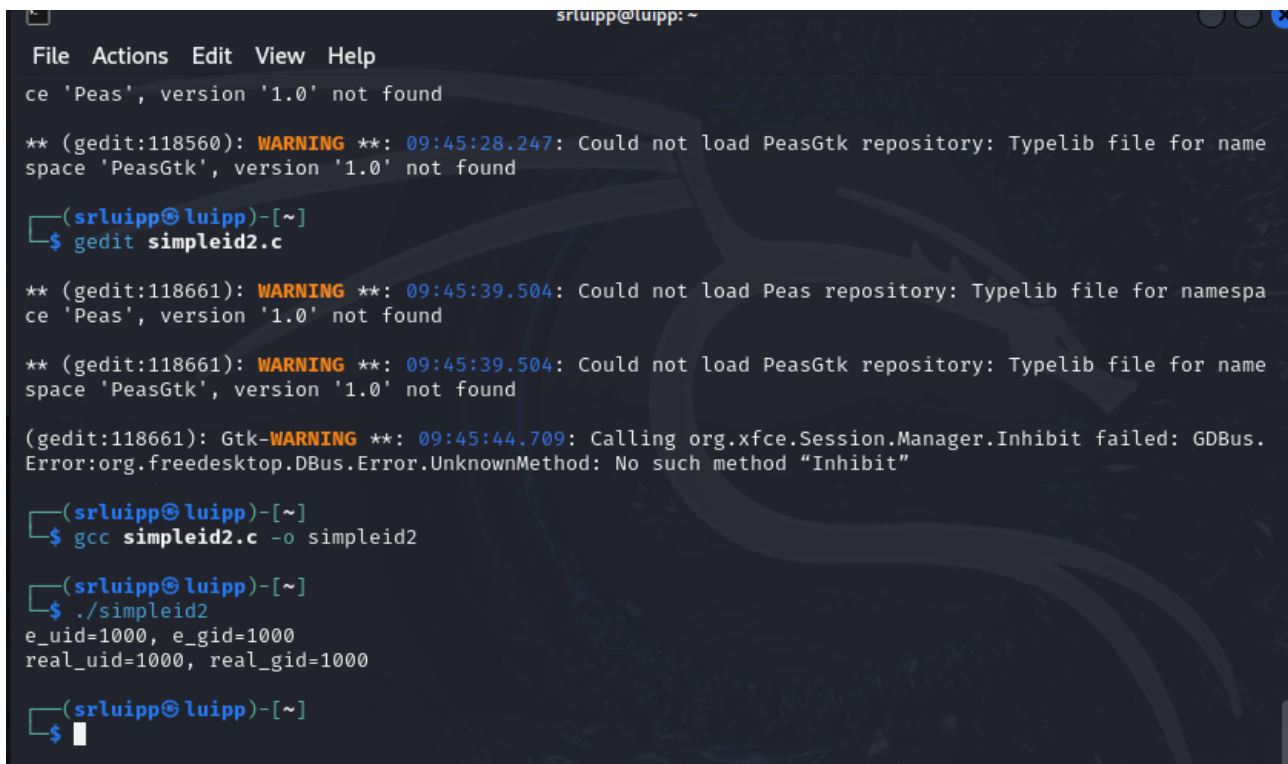
(gedit:118661): Gtk-WARNING **: 09:45:44. Error:org.freedesktop.DBus.Error.UnknownM
```

Создание и компиляция файла

C++ Листинг 3 #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; }
```

(рис. 12)



```
srluipp@luipp: ~  
File Actions Edit View Help  
ce 'Peas', version '1.0' not found  
  
** (gedit:118560): WARNING **: 09:45:28.247: Could not load PeasGtk repository: Typelib file for name  
space 'PeasGtk', version '1.0' not found  
  
(srluipp@luipp)-[~]  
$ gedit simpleid2.c  
  
** (gedit:118661): WARNING **: 09:45:39.504: Could not load Peas repository: Typelib file for namespa  
ce 'Peas', version '1.0' not found  
  
** (gedit:118661): WARNING **: 09:45:39.504: Could not load PeasGtk repository: Typelib file for name  
space 'PeasGtk', version '1.0' not found  
  
(gedit:118661): Gtk-WARNING **: 09:45:44.709: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.  
Error:org.freedesktop.DBus.Error.UnknownMethod: No such method "Inhibit"  
  
(srluipp@luipp)-[~]  
$ gcc simpleid2.c -o simpleid2  
  
(srluipp@luipp)-[~]  
$ ./simpleid2  
e_uid=1000, e_gid=1000  
real_uid=1000, real_gid=1000  
  
(srluipp@luipp)-[~]  
$
```

Содержимое файла

Снова от имени суперпользователя меняю владельца файла readfile. Далее меняю права доступа так, чтобы пользователь guest не смог прочесть содержимое файла (рис. 13)

```
srluipp@luipp: ~  
File Actions Edit View Help  
** (gedit:118661): WARNING **: 09:45:39.504: Could not load PeasGtk repository: Typelib file for name  
space 'PeasGtk', version '1.0' not found  
  
(gedit:118661): Gtk-WARNING **: 09:45:44.709: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.  
Error:org.freedesktop.DBus.Error.UnknownMethod: No such method "Inhibit"  
  
(srluipp@luipp)-[~]  
$ gcc simpleid2.c -o simpleid2  
  
(srluipp@luipp)-[~]  
$ ./simpleid2  
e_uid=1000, e_gid=1000  
real_uid=1000, real_gid=1000  
  
(srluipp@luipp)-[~]  
$ chown root:srluipp /home/srluipp/simpleid2  
chown: changing ownership of '/home/srluipp/simpleid2': Operation not permitted  
  
(srluipp@luipp)-[~]  
$ sudo chown root:srluipp /home/srluipp/simpleid2  
[sudo] password for srluipp:  
  
(srluipp@luipp)-[~]  
$ sudo chmod u+s /home/srluipp/simpleid2  
  
(srluipp@luipp)-[~]  
$
```

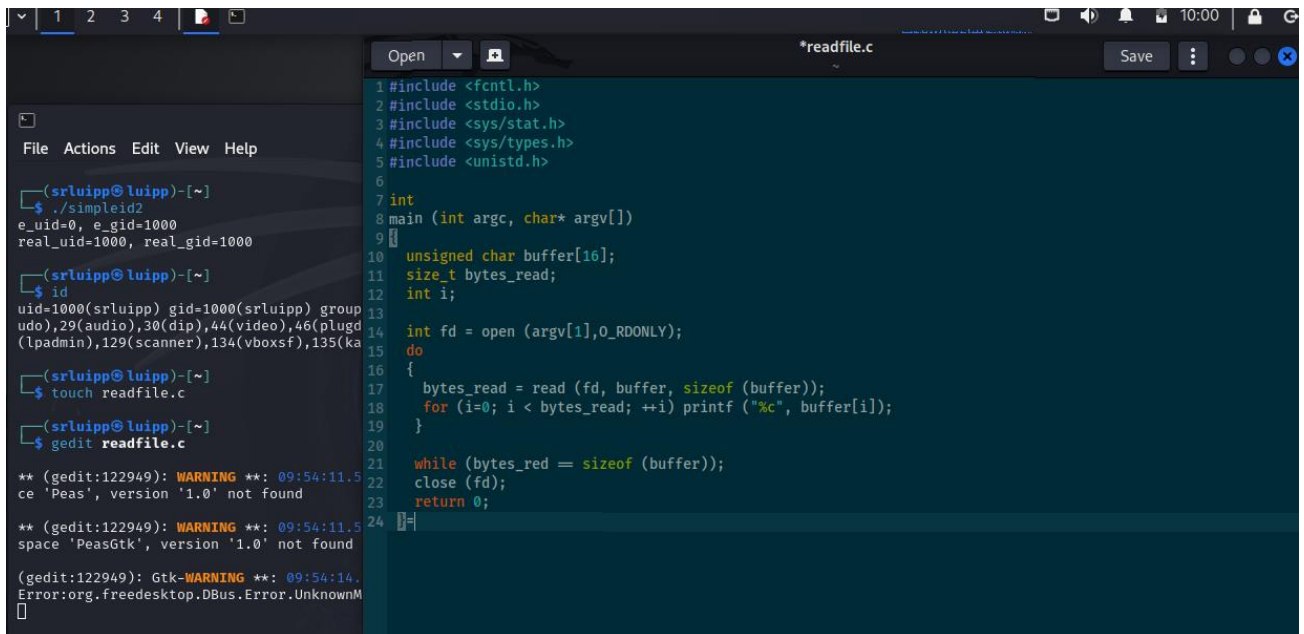
Смена владельца файла и прав доступа к файлу

Проверка прочесть файл от имени пользователя guest.Прочесть файл не удастся (рис. 14)

```
srluipp@luipp: ~  
File Actions Edit View Help  
$ chown root:srluipp /home/srluipp/simpleid2  
chown: changing ownership of '/home/srluipp/simpleid2': Operation not permitted  
  
(srluipp@luipp)-[~]  
$ sudo chown root:srluipp /home/srluipp/simpleid2  
[sudo] password for srluipp:  
  
(srluipp@luipp)-[~]  
$ sudo chmod u+s /home/srluipp/simpleid2  
  
(srluipp@luipp)-[~]  
$ ls -l simpleid2  
-rwsrwxr-x 1 root srluipp 16168 Apr 19 09:50 simpleid2  
  
(srluipp@luipp)-[~]  
$ ./simpleid2  
e_uid=0, e_gid=1000  
real_uid=1000, real_gid=1000  
  
(srluipp@luipp)-[~]  
$ id  
uid=1000(srluipp) gid=1000(srluipp) groups=1000(srluipp),4(adm),20(dialout),24(cdrom),25(floppy),27(s  
udo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),116(blueetooth),121(wireshark),123  
(lpadmin),129(scanner),134(vboxsf),135(kaboxer)  
  
(srluipp@luipp)-[~]  
$
```

Попытка прочесть содержимое файла

Попытка прочесть тот же файл с помощью программы readfile, в ответ получаем “отказано в доступе” (рис. 15)



```
1 #include <fcntl.h>
2 #include <stdio.h>
3 #include <sys/stat.h>
4 #include <sys/types.h>
5 #include <unistd.h>
6
7 int
8 main (int argc, char* argv[])
9 {
10     unsigned char buffer[16];
11     size_t bytes_read;
12     int i;
13
14     int fd = open (argv[1], O_RDONLY);
15     do
16     {
17         bytes_read = read (fd, buffer, sizeof (buffer));
18         for (i=0; i < bytes_read; ++i) printf ("%c", buffer[i]);
19     }
20     while (bytes_read == sizeof (buffer));
21     close (fd);
22     return 0;
23 }
```

```
(srluipp@luipp)-[~]
$ ./simpleid2
e_uid=0, e_gid=1000
real_uid=1000, real_gid=1000

(srluipp@luipp)-[~]
$ id
uid=1000(srluipp) gid=1000(srluipp) group
udo,29(audio),30(dip),44(video),46(plugd
(lpadmin),129(scanner),134(vboxsf),135(ka

(srluipp@luipp)-[~]
$ touch readfile.c

(srluipp@luipp)-[~]
$ gedit readfile.c

** (gedit:122949): WARNING **: 09:54:11.5
ce 'Peas', version '1.0' not found

** (gedit:122949): WARNING **: 09:54:11.5
space 'PeasGtk', version '1.0' not found

(gedit:122949): Gtk-WARNING **: 09:54:14.
Error:org.freedesktop.DBus.Error.UnknownM
```

4 Выводы

Изучила механизм изменения идентификаторов, применила SetUID- и Sticky-биты. Получила практические навыки работы в кон- соли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы