

Отчёт лабораторной работы 5

**Дискреционное разграничение прав в Linux. Исследование влияния
дополнительных атрибутов**

Турсунов Баходурхон Азимджонович

Содержание

1	Цель работы	5
1.1	2.1 Подготовка лабораторного стенда	5
1.2	2.2 Изучение механики SetUID	6
1.3	2.3 Исследование Sticky-бита	10
2	Вывод	12

List of Figures

1.1	gcc	5
1.2	gcc -v	6
1.3	simpleid.c	6
1.4	результат программы simpleid	7
1.5	программа simpleid2	7
1.6	результат программы simpleid2	8
1.7	программа readfile.c	8
1.8	результат программы readfile.c	9
1.9	результат программы readfile.c	9
1.10	исследование Sticky-бита	10
1.11	исследование Sticky-бита	10
1.12	чтение и запись на файл	11
1.13	чтение и запись на файл	11

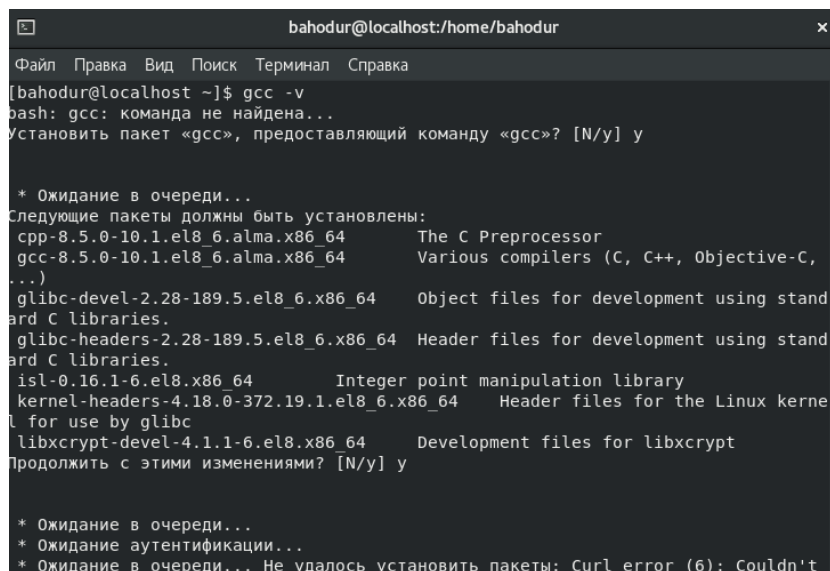
List of Tables

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.

1.1 2.1 Подготовка лабораторного стенда

1. С помощью команды `gcc -v` проверил, установлен ли компилятор gcc в моей системе, как оказалось не установлен



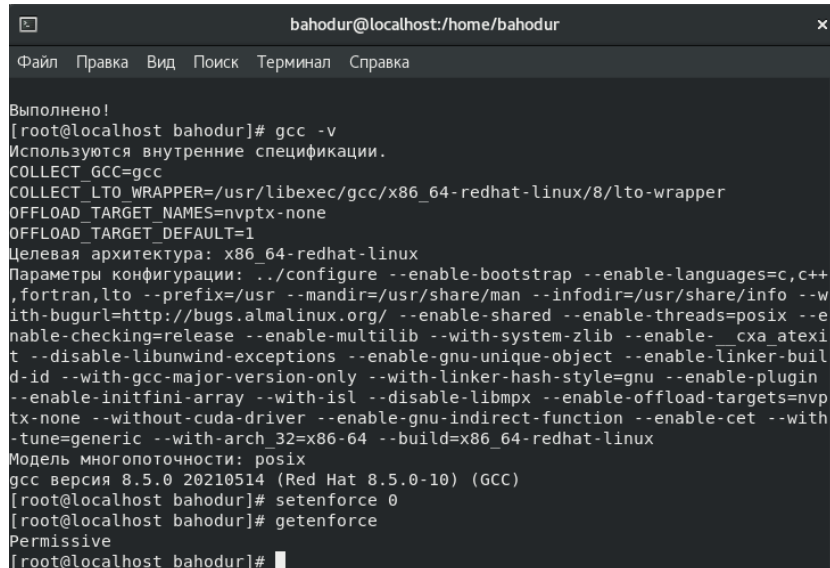
```
bahodur@localhost:~/home/bahodur
[bahodur@localhost ~]$ gcc -v
bash: gcc: команда не найдена...
Установить пакет «gcc», предоставляющий команду «gcc»? [N/y] y

* Ожидание в очереди...
Следующие пакеты должны быть установлены:
gcc-8.5.0-10.1.el8_6.alma.x86_64      The C Preprocessor
gcc-8.5.0-10.1.el8_6.alma.x86_64      Various compilers (C, C++, Objective-C,
...)
glibc-devel-2.28-189.5.el8_6.x86_64  Object files for development using stand
ard C libraries.
glibc-headers-2.28-189.5.el8_6.x86_64 Header files for development using stand
ard C libraries.
isl-0.16.1-6.el8.x86_64              Integer point manipulation library
kernel-headers-4.18.0-372.19.1.el8_6.x86_64 Header files for the Linux kerne
l for use by glibc
libxcrypt-devel-4.1.1-6.el8.x86_64    Development files for libxcrypt
Продолжить с этими изменениями? [N/y] y

* Ожидание в очереди...
* Ожидание аутентификации...
* Ожидание в очереди... Не удалось установить пакеты: Curl error (6): Couldn't
```

Figure 1.1: gcc

2. После установления компилятора gcc с помощью команды `gcc -v` узнаем подробности и версию нашего компилятора, затем отключил систему запретов до очередной перезагрузки системы командой `setenforce 0`, после этого команда `getenforce` вывела `Permissive`.

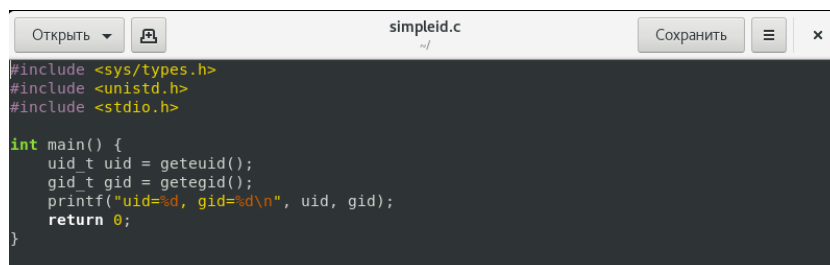


```
Выполнено!
[root@localhost bahodur]# gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/8/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --enable-languages=c,c++
,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --w
ith-bugurl=http://bugs.almalinux.org/ --enable-shared --enable-threads=posix --e
nable-checking=release --enable-multilib --with-system-zlib --enable-__cxa_atexi
t --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-buil
d-id --with-gcc-major-version-only --with-linker-hash-style=gnu --enable-plugin
--enable-initfini-array --with-isl --disable-libmpx --enable-offload-targets=nvp
tx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with
-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Модель многопоточности: posix
gcc версия 8.5.0 20210514 (Red Hat 8.5.0-10) (GCC)
[root@localhost bahodur]# setenforce 0
[root@localhost bahodur]# getenforce
Permissive
[root@localhost bahodur]#
```

Figure 1.2: gcc -v

1.2 2.2 Изучение механики SetUID

1. Вошел в систему от имени пользователя guest
2. Написал программу simpleid.c

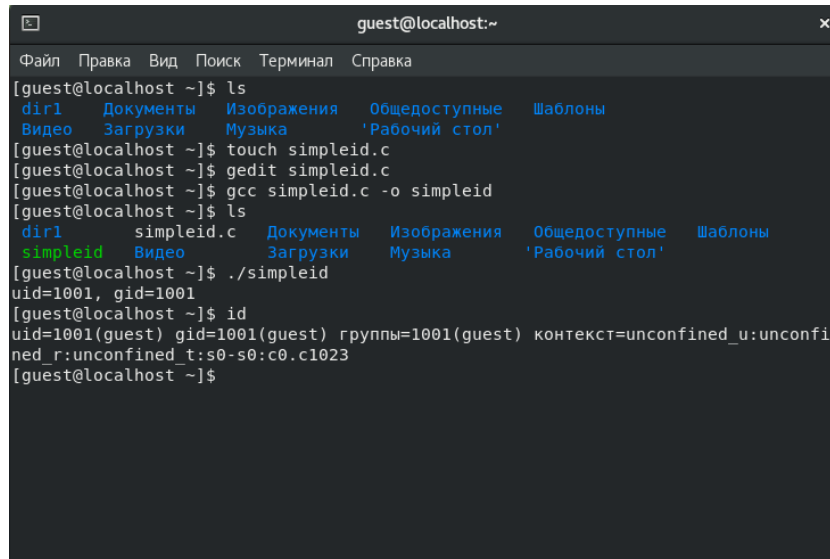


```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main() {
    uid_t uid = getuid();
    gid_t gid = getegid();
    printf("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Figure 1.3: simpleid.c

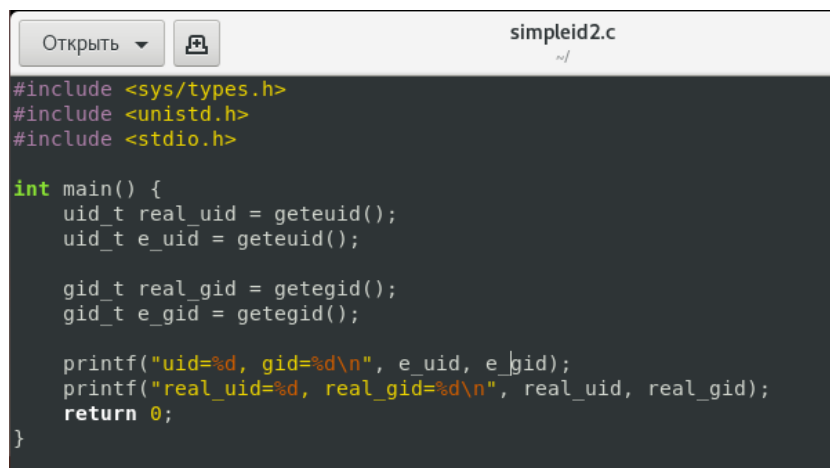
3. Скомпилировал программу и убедился, что файл программы создан с помощью команды `gcc simpleid.c -o simpleid`
4. Далее выполнил программу `simpleid` командой `./simpleid`
5. Выполнил системную программу `id` с помощью команды `id`. `uid` и `gid` совпадает в обеих программах



```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ ls  
dir1  Документы  Изображения  Общедоступные  Шаблоны  
Видео  Загрузки  Музыка  'Рабочий стол'  
[guest@localhost ~]$ touch simpleid.c  
[guest@localhost ~]$ gedit simpleid.c  
[guest@localhost ~]$ gcc simpleid.c -o simpleid  
[guest@localhost ~]$ ls  
dir1  simpleid.c  Документы  Изображения  Общедоступные  Шаблоны  
simpleid  Видео  Загрузки  Музыка  'Рабочий стол'  
[guest@localhost ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$
```

Figure 1.4: результат программы `simpleid`

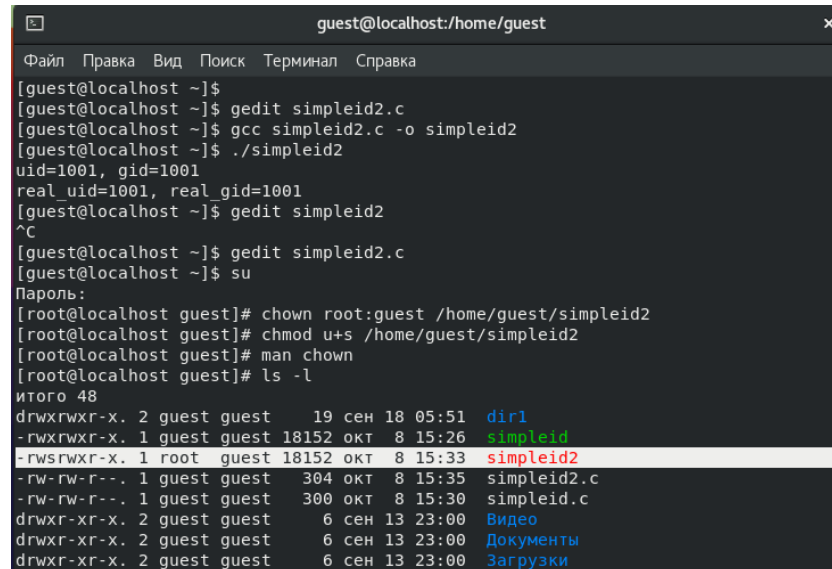
6. Усложнил программу, добавив вывод действительных идентификаторов



```
simpleid2.c  
~/  
#include <sys/types.h>  
#include <unistd.h>  
#include <stdio.h>  
  
int main() {  
    uid_t real_uid = geteuid();  
    uid_t e_uid = geteuid();  
  
    gid_t real_gid = getegid();  
    gid_t e_gid = getegid();  
  
    printf("uid=%d, gid=%d\n", e_uid, e_gid);  
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);  
    return 0;  
}
```

Figure 1.5: программа `simpleid2`

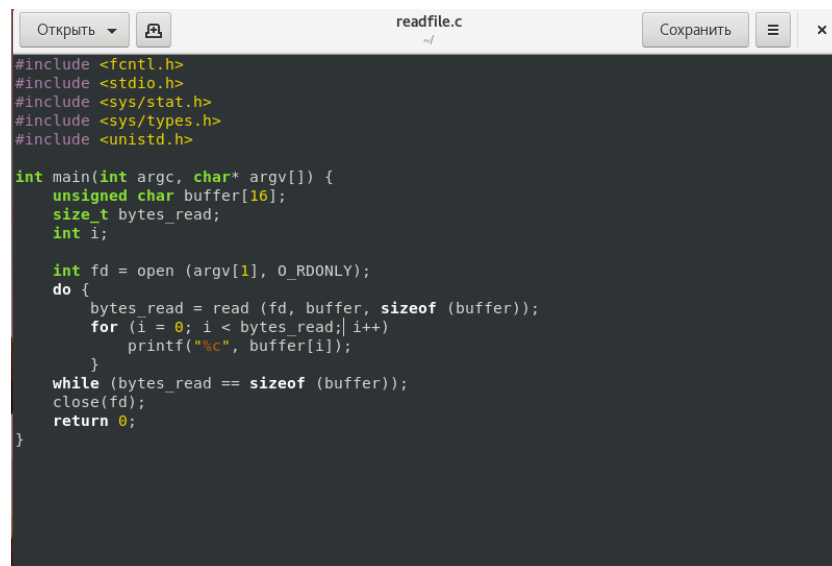
7. Далее скомпилировал и запустил simpleid2.c и от имени суперпользователя выполнил команды chown и chmod u+s и выполнил проверку правильности установки новых атрибутов и имени владельца файла



```
guest@localhost:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@localhost ~]$
[guest@localhost ~]$ gedit simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
uid=1001, gid=1001
real uid=1001, real gid=1001
[guest@localhost ~]$ gedit simpleid2
^C
[guest@localhost ~]$ gedit simpleid2.c
[guest@localhost ~]$ su
Пароль:
[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]# man chown
[root@localhost guest]# ls -l
итого 48
drwxrwxr-x. 2 guest guest 19 сен 18 05:51 dir1
-rwxrwxr-x. 1 guest guest 18152 окт 8 15:26 simpleid
-rwsrwxr-x. 1 root guest 18152 окт 8 15:33 simpleid2
-rw-rw-r--. 1 guest guest 304 окт 8 15:35 simpleid2.c
-rw-rw-r--. 1 guest guest 300 окт 8 15:30 simpleid.c
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Загрузки
```

Figure 1.6: результат программы simpleid2

8. Написал программы readfile.c



```
Открыть readfile.c Сохранить
#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;
}
```

Figure 1.7: программа readfile.c

9. Скомпилировал файл

```
[guest@localhost ~]$ gedit readfile.c  
[guest@localhost ~]$ gcc readfile.c -o readfile  
[guest@localhost ~]$ ./readfile  
@@000000000000000000E00~000+0000+00GZ00<;d0c0000000+0<;D      E0<;*0K00  
000+00!000~-  
00-0c000+00c000+0g 000~000+0000+000  
0+0 '  
0+08  
0+0M  
0+0d  
0+0o  
0+00  
0+00  
0+00  
0+00  
0+00  
0+00  
0+0  
0+000  
0+00
```

Figure 1.8: результат программы readfile.c

10. Сменил владельца у файла и изменил права так, чтобы только суперпользователь мог прочитать его, а guest не мог. И проверил что пользователю отказано в доступе и он не может прочитать файл.

```
[guest@localhost ~]$ su
Пароль:
[root@localhost guest]# ls -l
итого 96
-rwxrwxr-x. 1 guest guest 18200 ОКТ 8 15:54 a.out
drwxrwxr-x. 2 guest guest 19 сен 18 05:51 dir1
-rwxrwxr-x. 1 guest guest 18200 ОКТ 8 15:53 readfile
----- 1 bahodur bahodur 420 ОКТ 8 15:58 readfile.c
-rwxrwxr-x. 1 guest guest 18152 ОКТ 8 15:26 simpleid
-rwsrwxr-x. 1 root guest 18152 ОКТ 8 15:33 simpleid2
-rw-rw-r--. 1 guest guest 304 ОКТ 8 15:35 simpleid2.c
-rw-rw-r--. 1 guest guest 300 ОКТ 8 15:30 simpleid.c
-rw-r--r--. 1 root root 418 ОКТ 8 15:50 txt.txt
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Изображения
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Музыка
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 13 23:00 Шаблоны
[root@localhost guest]# exit
exit
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@localhost ~]$
```

Figure 1.9: результат программы readfile.c

1.3 2.3 Исследование Sticky-бита

1. Выяснил, установлен ли атрибут Sticky на директории /tmp.
2. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test.
3. Просмотрел атрибут у только что созданного файла и разрешил чтение и запись для категории пользователей “все остальные”

```
[guest@localhost ~]$ ls -l / | grep tmp
drwxrwxrwt. 15 root root 4096 окт  8 16:06 tmp
[guest@localhost ~]$ echo "test" >> /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 окт  8 16:13 /tmp/file01.txt
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt
```

Figure 1.10: исследование Sticky-бита

- Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме “остальных пользователей”

```
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  8 16:13 /tmp/file01.txt
```

Figure 1.11: исследование Sticky-бита

4. От пользователя (не являющегося владельцем) попробовал прочитать файл /file01.txt
5. От пользователя попробовал записал в файл test и test2 и проверил командой cat /tmp/file01.txt

```

[guest@localhost home]$ su guest2
Пароль:
[guest2@localhost home]$ ls
bahodur guest guest2
[guest2@localhost home]$ cd guest
[guest2@localhost guest]$ ls
a.out      simpleid      txt.txt      Изображения  Шаблоны
dir1       simpleid2     Видео        Музыка
readfile   simpleid2.c   Документы    Общедоступные
readfile.c simpleid.c     Загрузки     'Рабочий стол'
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test
test2
[guest2@localhost guest]$

```

Figure 1.12: чтение и запись на файл

- И убеждаемся, что в файле действительно есть наши записанные слова.
6. От пользователя попробовал записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию. И командой echo "test3" » /tmp/file01.txt записал новую информацию в файл
 7. Также проверил информацию, которая лежит в файле командой cat /tmp/file01.txt
 8. От пользователя попробовал удалить файл, и получил отказ
 9. От имени суперпользователя выполнил команду, снимающую атрибут t с директории /tmp и покинул режим суперпользователя
 10. Повторил предыдущие шаги и мне удалось удалить файл

```

guest2@localhost:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest2@localhost guest]$ echo "test3" >> /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@localhost guest]$ su -
Пароль:
[root@localhost ~]# chmod -t /tmp
[root@localhost ~]# exit
выход
[guest2@localhost guest]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 окт  8 16:20 tmp
[guest2@localhost guest]$ rm /tmp/file01.txt
[guest2@localhost guest]$

```

Figure 1.13: чтение и запись на файл

2 Вывод

- Изучил механизмы изменение идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Также рассмотрел работу механизма смены идентификатора процессов пользователей и влияние бита на запись и удаление файлов.