

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

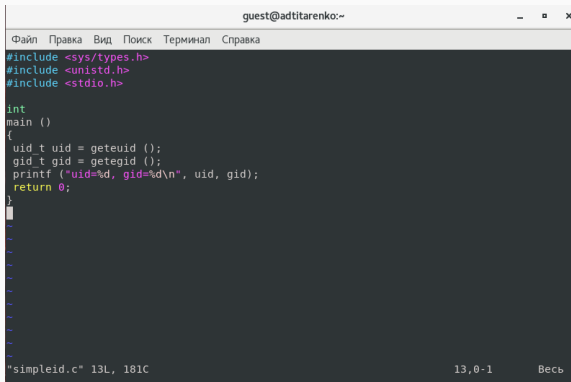
Титаренко Анастасия НПИбд-02-19¹

2022, 8 October, Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

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.

Листинг программы simpleid.c



The image shows a screenshot of a code editor window. The title bar at the top reads "guest@adtitarenko:~". Below the title bar is a menu bar with the following items: "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The main area of the window contains the following C code:

```
#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;
}
```

At the bottom of the window, there is a status bar that displays the filename and line/column information: "simpleid.c" 13L, 181C. On the right side of the status bar, it shows "13,0-1" and "Весь".

Рис. 1: Листинг программы simpleid.c

Компилирование программы simpleid.c

```
[guest@adtitarenko ~]$ gcc simpleid.c -o simpleid  
[guest@adtitarenko ~]$ ls  
dir1 simpleid simpleid.c  
[guest@adtitarenko ~]$
```

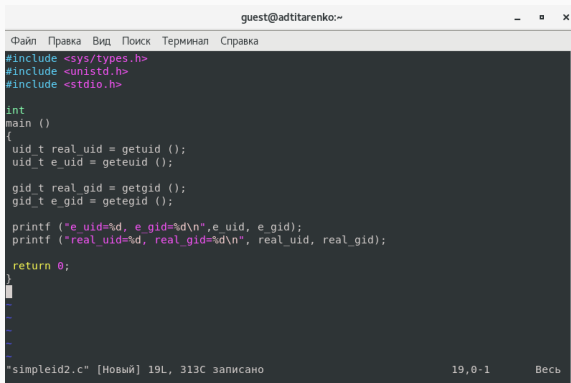
Рис. 2: Компилирование программы simpleid.c

Сравнение результата команд ./simpleid и id

```
[guest@adtitarenko ~]$ ./simpleid
uid=1001, gid=1001
[guest@adtitarenko ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 3: Сравнение результата команд ./simpleid и id

Листинг программы simpleid2.c



```
guest@adtitarenko:~
Файл  Правка  Вид  Поиск  Терминал  Справка

#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;
}

simpleid2.c" [Новый] 19L, 313C записано    19,0-1    Весь
```

Рис. 4: Листинг программы simpleid2.c

Компилирование и запуск программы simpleid2.c

```
[guest@adtitarenko ~]$ gcc simpleid2.c -o simpleid2  
[guest@adtitarenko ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real uid=1001, real gid=1001
```

Рис. 5: Компилирование и запуск программы simpleid2.c

Изменение прав доступа файла simpleid2

```
[root@adtitarenko ~]# chown root:guest /home/guest/simpleid2  
[root@adtitarenko ~]# chmod u+s /home/guest/simpleid2  
[root@adtitarenko ~]#
```

Рис. 6: Изменение прав доступа файла simpleid2

Проверка правильности установки новых атрибутов и смены владельца файла simpleid2

```
[root@adtitarenko guest]#  
[root@adtitarenko guest]# ls -l simpleid2  
-rwsrwxr-x. 1 root guest 8616 окт  8 18:09 simpleid2  
[root@adtitarenko guest]#
```

Рис. 7: Проверка правильности установки новых атрибутов и смены владельца файла simpleid2

Сравнение результата команд ./simpleid2 и id

```
[root@adtitarenko guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@adtitarenko guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
```

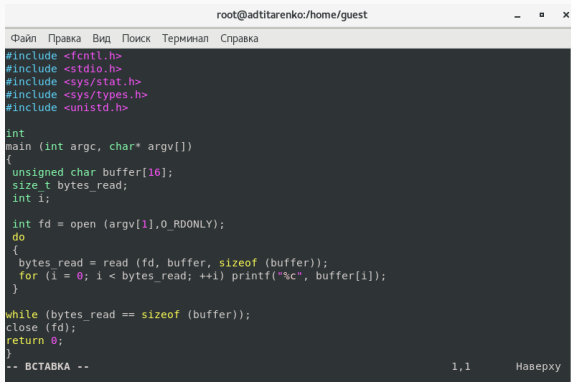
Рис. 8: Сравнение результата команд ./simpleid2 и id

Изменения относительно SetGID-бита файла simpleid2

```
[root@adtitarenko guest]# chmod g+s /home/guest/simpleid2
[root@adtitarenko guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 8616 окт  8 18:09 simpleid2
[root@adtitarenko guest]# ./simpleid2
e_uid=0, e_gid=1001
real uid=0, real gid=0
```

Рис. 9: Изменения относительно SetGID-бита файла simpleid2

Листинг программы readfile.c



```
root@adtitarenko:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка

#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;
}
-- ВСТАВКА --                                     1,1      Наверх
```

Рис. 10: Листинг программы readfile.c

```
[root@adtitarenko guest]#  
[root@adtitarenko guest]#  
[root@adtitarenko guest]# gcc readfile.c -o readfile
```

Рис. 11: Компилирование программы readfile.c

Изменения прав файла readfile.c

```
[root@adtitarenko guest]#  
[root@adtitarenko guest]#  
[root@adtitarenko guest]# chown root readfile.c  
[root@adtitarenko guest]# chmod og-rwx readfile.c  
[root@adtitarenko guest]#  
[root@adtitarenko guest]# su - guest  
Последний вход в систему: C6 окт  8 17:52:24 MSK 2022 на pts/0  
[guest@adtitarenko ~]$  
[guest@adtitarenko ~]$ cat readfile.c  
cat: readfile.c: Отказано в доступе
```

Рис. 12: Изменения прав файла readfile.c

Установка SetU'D-бита и изменения владельца файла readfile.c

```
[root@adtitarenko guest]# chmod u+s /home/guest/readfile
[root@adtitarenko guest]# ./readfile
[0s0zlm[0 @0#000s0Z+100[s0 090SZ0)0i[0a[0[0[0[0#000I@0#000[0[0]'0009'000D'000U'000j'000~'
0000'0000'0000'000 0000.0000.0000.0000.000[000 /000/0007/000[0000/0000/000!0000[000
[0000[0000[0000[000i[00 @
```

Рис. 13: Установка SetU'D-бита и изменения владельца файла readfile.c

Выполнение команды: `ls -l / | grep tmp`

```
[root@adtitarenko guest]# ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 окт  8 18:34 tmp
[root@adtitarenko guest]#
[root@adtitarenko guest]# su - guest
Последний вход в систему: C6 окт  8 18:33:35 MSK 2022 на pts/0
[guest@adtitarenko ~]$
```

Рис. 14: Выполнение команды: `ls -l / | grep tmp`

Создание файла file01.txt

```
[guest@adtitarenko ~]$  
[guest@adtitarenko ~]$ echo "test" > /tmp/file01.txt  
[guest@adtitarenko ~]$  
[guest@adtitarenko ~]$ ls /tmp  
anaconda.log  
file01.txt
```

Рис. 15: Создание файла file01.txt

Просмотр атрибутов и изменение прав файла file01.txt

```
[guest@adtitarenko ~]$  
[guest@adtitarenko ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 окт  8 18:38 /tmp/file01.txt  
[guest@adtitarenko ~]$ chmod o+rw /tmp/file01.txt  
[guest@adtitarenko ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 окт  8 18:38 /tmp/file01.txt  
[guest@adtitarenko ~]$
```

Рис. 16: Просмотр атрибутов и изменение прав файла file01.txt

Попытка прочитать файл file01.txt от пользователя, не являющегося владельцем

```
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$ cat /tmp/file01.txt  
test
```

Рис. 17: Попытка прочитать файл file01.txt от пользователя, не являющегося владельцем

Изменение файла file01.txt и просмотр содержимого

```
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$ cat /tmp/file01.txt  
test2  
[guest2@adtitarenko ~]$
```

Рис. 18: Изменение файла file01.txt и просмотр содержимого

Изменение файла file01.txt и просмотр содержимого

```
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$ echo "test3" > /tmp/file01.txt  
[guest2@adtitarenko ~]$ cat /tmp/file01.txt  
test3
```

Рис. 19: Изменение файла file01.txt и просмотр содержимого

Попытка удалить файл file01.txt]

```
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$ rm /tmp/file01.txt  
rm: невозможно удалить «/tmp/file01.txt»: Операция не позволена
```

Рис. 20: Попытка удалить файл file01.txt

Сняла атрибут -t с директории /tmp и покинула режим суперпользователя

```
[guest2@adtitarenko ~]$ su
Пароль:
[root@adtitarenko guest2]# chmod -t /tmp
[root@adtitarenko guest2]# exit
exit
```

Рис. 21: Сняла атрибут -t с директории /tmp и покинула режим суперпользователя

Проверка: атрибута -t нет у директории /tmp

```
[guest2@adtitarenko ~]$ ls -l / | grep tmp  
drwxrwxrwx. 17 root root 4096 окт 8 18:44 tmp  
[guest2@adtitarenko ~]$  
[guest2@adtitarenko ~]$
```

Рис. 22: Проверка: атрибута -t нет у директории /tmp

```
[guest2@adtitarenko ~]$ cat /tmp/file01.txt
test3
[guest2@adtitarenko ~]$ echo "test2" > /tmp/file01.txt
[guest2@adtitarenko ~]$ cat /tmp/file01.txt
test2
[guest2@adtitarenko ~]$ echo "test3" > /tmp/file01.txt
[guest2@adtitarenko ~]$ cat /tmp/file01.txt
test3
[guest2@adtitarenko ~]$ rm /tmp/file01.txt
[guest2@adtitarenko ~]$
```

Рис. 23: Повтор предыдущих шагов

Вернула атрибут -t с директории /tmp

```
[root@adtitarenko guest2]# chmod +t /tmp  
[root@adtitarenko guest2]# exit  
exit  
[guest2@adtitarenko ~]$
```

Рис. 24: Вернула атрибут -t с директории /tmp

Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. 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.