

Лабораторная работа №5

Аминов Зулфикор¹

8.10, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

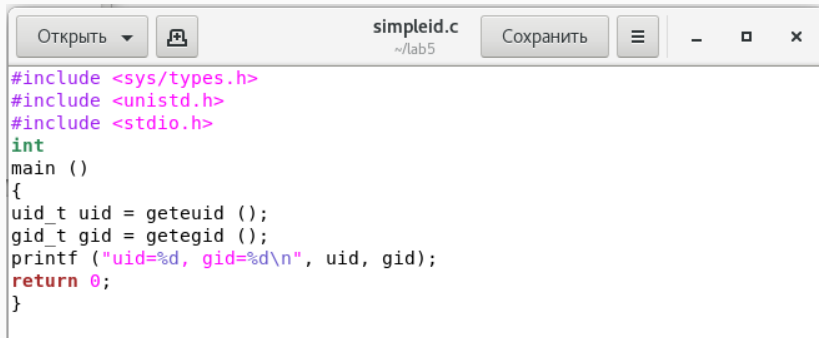
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Выполнение работы

Вошли в систему от имени пользователя guest

Создали файл simpleid.c:

```
[guest@zulfikor ~]$ cd lab5/  
[guest@zulfikor lab5]$ > simpleid.c  
[guest@zulfikor lab5]$ gedit simpleid.c
```



```
#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;  
}
```

Скомпилировали программу

```
[guest@zulfikor lab5]$ gcc simpleid.c -o simpleid  
[guest@zulfikor lab5]$
```

Запустили программу simpleid

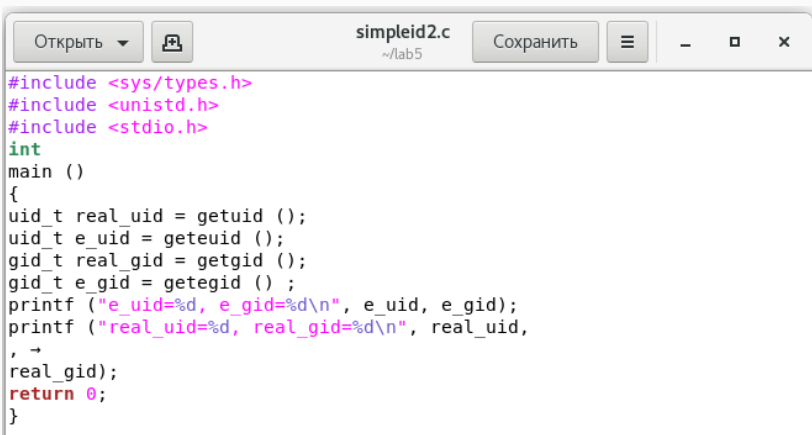
```
[guest@zulfikor lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@zulfikor lab5]$
```

Выполнили системную программу id

```
[guest@zulfikor lab5]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@zulfikor lab5]$
```


Создали файл simpleid2.c

```
[guest@zulfikor lab5]$ > simpleid2.c  
[guest@zulfikor lab5]$ gedit simpleid2.c
```



```
#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;  
}
```

Скомпилировали и запустили simpleid2.c

```
[guest@zulfikor lab5]$ gcc simpleid2.c -o simpleid2
[guest@zulfikor lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@zulfikor lab5]$ █
```

От имени суперпользователя выполнили команды

```
guest@zulfikor:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@zulfikor ~]$ su
Пароль:
[root@zulfikor guest]# chown root:guest /home/guest/simpleid2
chown: невозможно получить доступ к «/home/guest/simpleid2»: Нет такого файла или
[root@zulfikor guest]# chown root:guest /home/guest/lab5/simpleid2
[root@zulfikor guest]# chmod u+s /home/guest/lab5/simpleid2
[root@zulfikor guest]#
```

Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2

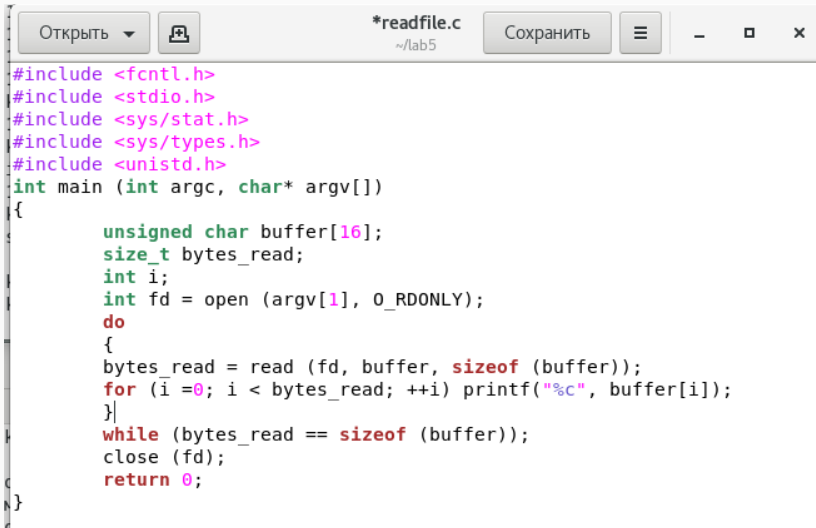
```
[guest@zulfikor lab5]$ ls -l
итого 32
-rwxrwxr-x. 1 guest guest 8472 окт  8 18:39 simpleid
-rwsrwxr-x. 1 root  guest 8576 окт  8 18:42 simpleid2
-rw-rw-r--. 1 guest guest  303 окт  8 18:41 simpleid2.c
-rw-rw-r--. 1 guest guest  175 окт  8 18:39 simpleid.c
[guest@zulfikor lab5]$
```

Запустили simpleid2 и id:

```
[guest@zulfikor lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@zulfikor lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Создали файл readfile.c

```
[guest@zulfikor lab5]$ > readfile.c  
[guest@zulfikor lab5]$ gedit readfile.c
```



```
#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;
}
```

Откомпилировали программу

```
~guest@zulfikor lab5]$ gcc readfile.c -o readfile  
~guest@zulfikor lab5]$
```

Сменили владельца у файла readfile.c и измените права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог

```
[root@zulfikor guest]# chown root:guest /home/guest/lab5/readfile.c  
[root@zulfikor guest]# chmod 400 /home/guest/lab5/readfile.c  
[root@zulfikor guest]# █
```


Проверили, что пользователь guest не может ли прочитать файл readfile.c.

```
[guest@zulfikor lab5]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@zulfikor lab5]$
```

Сменили у программы readfile владельца и установите SetU'D-бит

```
[root@zulfikor guest]# chown root:guest /home/guest/lab5/readfile
[root@zulfikor guest]# chmod u+s /home/guest/lab5/readfile
[root@zulfikor guest]#
```

```
[guest@zulfikor lab5]$ ls -l
итого 48
-rwsrwxr-x. 1 root  guest 8512 окт  8 18:47 readfile
-r----- 1 root  guest  414 окт  8 18:47 readfile.c
-rwxrwxr-x. 1 guest guest 8472 окт  8 18:39 simpleid
-rwsrwxr-x. 1 root  guest 8576 окт  8 18:42 simpleid2
-rw-rw-r-- 1 guest guest  303 окт  8 18:41 simpleid2.c
-rw-rw-r-- 1 guest guest  175 окт  8 18:39 simpleid.c
[guest@zulfikor lab5]$
```

Проверка, может ли программа readfile прочитать файл readfile.c?

```
[guest@zulfikor lab5]$ ./readfile readfile.c
#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;
}
[guest@zulfikor lab5]$
```

Проверили, может ли программа readfile прочитать файл /etc/shadow

```
[guest@zulfikor lab5]$ ./readfile /etc/shadow
root:$6$ZlSroY.K/docyJaG$xsuFtcJrUNazlh4z7aBT/b49d4YY9n8SQo4wUGdAz0q4ZreTHEApDPns0Xe0Mr
yRNqfgaU1::0:99999:7:::
bin*:18353:0:99999:7:::
daemon*:18353:0:99999:7:::
adm*:18353:0:99999:7:::
lp*:18353:0:99999:7:::
sync*:18353:0:99999:7:::
shutdown*:18353:0:99999:7:::
halt*:18353:0:99999:7:::
mail*:18353:0:99999:7:::
operator*:18353:0:99999:7:::
games*:18353:0:99999:7:::
ftp*:18353:0:99999:7:::
nobody*:18353:0:99999:7:::
systemd-network:!!:19245:::
dbus:!!:19245:::
polkitd:!!:19245:::
libstoragemgmt:!!:19245:::
```

Исследование Sticky-бита

Выяснили, установлен ли атрибут Sticky на директории /tmp

```
guest@zulfikor:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@zulfikor ~]$ ls -l / | grep tmp  
drwxrwxrwt. 34 root root 8192 окт  8 18:53 tmp  
[guest@zulfikor ~]$
```

От имени пользователя guest создали файл file01.txt в директории /tmp со словом test

```
[guest@zulfikor ~]$ echo "test" > /tmp/file01.txt  
[guest@zulfikor ~]$
```

Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»

```
[guest@zulfikor ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 окт  8 18:55 /tmp/file01.txt
[guest@zulfikor ~]$ chmod o+rw /tmp/file01.txt
[guest@zulfikor ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  8 18:55 /tmp/file01.txt
[guest@zulfikor ~]$
```


От пользователя guest2 попробовали прочитать файл /tmp/file01.txt

```
[guest@zulfikor ~]$ su guest2
Пароль:
[guest2@zulfikor guest]$ cat /tmp/file01.txt
test
[guest2@zulfikor guest]$ █
```

От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2

```
[guest2@zulfikor guest]$ echo "test2" >> /tmp/file01.txt  
[guest2@zulfikor guest]$
```

Проверили содержимое файла

```
[guest2@zulfikor guest]$ cat /tmp/file01.txt  
test  
test2  
[guest2@zulfikor guest]$
```

От пользователя `guest2` попробовали записать в файл `/tmp/file01.txt` слово `test3`, стеревав при этом всю имеющуюся в файле информацию

```
-----  
[guest2@zulfikor guest]$ echo "test3" > /tmp/file01.txt  
[guest2@zulfikor guest]$
```

Проверили содержимое файла

```
[guest2@zulfikor ~]$ cat /tmp/file01.txt  
test3  
[guest2@zulfikor ~]$
```

От пользователя guest2 попробовали удалить файл /tmp/file01.txt

```
[guest2@zulfikor guest]$ rm /tmp/file01.txt  
rm: невозможно удалить «/tmp/file01.txt»: Нет такого файла или каталога  
[guest2@zulfikor guest]$ █
```

От имени суперпользователя снимали атрибут t (Sticky-бит) с директории /tmp

```
[guest2@zulfikor guest]$ su
Пароль:
[root@zulfikor guest]# chmod -t /tmp
[root@zulfikor guest]#
```

Покинули режим суперпользователя

```
[root@zulfikor ~]# exit  
exit  
[guest2@zulfikor ~]$
```


От пользователя `guest2` проверили, что атрибута `t` у директории `/tmp` нет

```
[guest2@zulfikor guest]$ ls -l / | grep tmp  
drwxrwxrwx. 34 root root 8192 окт  8 19:00 tmp  
[guest2@zulfikor guest]$
```

Повторили предыдущие шаги

```
[guest2@zulfikor guest]$ rm /tmp/file0l.txt  
rm: невозможно удалить «/tmp/file0l.txt»: Нет такого файла или каталога
```

Не удалось удалить файл от имени пользователя

```
[root@zulfikor guest]# exit  
exit  
[guest2@zulfikor guest]$ █
```

Выводы по проделанной работе

Изучили механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практических навыков работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей.