

Лабораторная работа №5

Основы информационной безопасности

Павлюченков С.В.

07 сентября 25

Российский университет дружбы народов, Москва, Россия

- Павлюченков Сергей Витальевич
- Студент ФФМиЕН
- Российский университет дружбы народов
- 1132237372@pfur.ru
- <https://serapshi.github.io/svpavliuchenkov.github.io/>



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

Задание

Войдите как guest.

Создайте и скомпилируйте simpleid.c.

Запустите simpleid и проверьте идентификаторы с помощью команды id.

Усложните программу и запустите simpleid2.

Проверьте атрибуты для simpleid2.

Скомпилируйте readfile.c.

Смените владельца и атрибуты файла на readfile.

Создайте файл file01.txt в /tmp.

Проверьте доступ пользователя guest2 к файлу.

Снимите атрибут Sticky с /tmp

Выполнение лабораторной работы

```
[guest@svpavliuchenkov lab05]$ cat 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;
}
[guest@svpavliuchenkov lab05]$
```

Рис. 1: Листинг simpleid

```
simpleid.c      .simpleid.c.swp
[guest@svpavliuchenkov lab05]$ gcc simpleid.c -o simpleid
[guest@svpavliuchenkov lab05]$ ./simpleid
uid=1001, gid=1001
[guest@svpavliuchenkov lab05]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfi
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@svpavliuchenkov lab05]$
```

Рис. 2: Компиляция файл



```
mc [guest@svpavliuchenkov]:~/Desktop/lab05
File Edit View Search Terminal Help
simpleid.c [----] 6 L:[ 1+ 8 9/ 17] *(151 / 344b) 0100
#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 ("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;
}
```

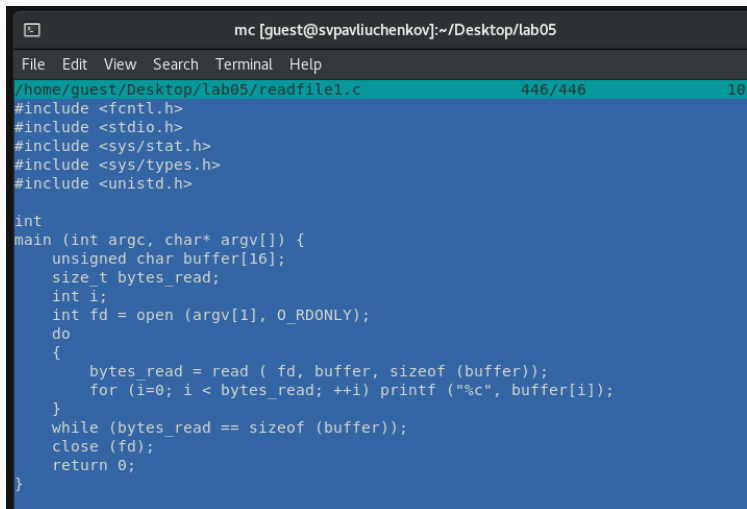
Рис. 3: Усложненный simpleid


```
[guest@svpavliuchenkov lab05]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest 18208 Sep 13 21:21 simpleid2  
[guest@svpavliuchenkov lab05]$
```

Рис. 4: Проверка атрибутов

```
[guest@svpavliuchenkov lab05]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=1001
[guest@svpavliuchenkov lab05]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@svpavliuchenkov lab05]$
```

Рис. 5: Компиляция и запуск simpleid2.c



```
mc [guest@svpavliuchenkov]:~/Desktop/lab05
File Edit View Search Terminal Help
/home/guest/Desktop/lab05/readfile1.c 446/446 10
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

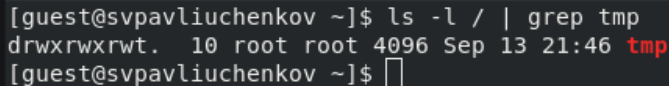
int
main (int argc, char* argv[]) {
    unsigned char buffer[16];
    size_t bytes_read;
    int i;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read ( fd, buffer, sizeof (buffer));
        for (i=0; i < bytes_read; ++i) printf ("%c", buffer[i]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

Рис. 6: Создание

```
[root@svpavliuchenko ~]# chown root:guest /home/guest/Desktop/lab05/readfile1.  
[root@svpavliuchenko ~]# chmod -r /home/guest/Desktop/lab05/readfile1.c  
[root@svpavliuchenko ~]# chmod u+s /home/guest/Desktop/lab05/readfile1.c  
[root@svpavliuchenko ~]#
```

Рис. 7: Команда chown guest:root

Проверяем папку tmp на наличие атрибута Sticky, т.к. в выводе есть буква t, то атрибут установлен



```
[guest@svpavliuchenv ~]$ ls -l / | grep tmp
drwxrwxrwt. 10 root root 4096 Sep 13 21:46 tmp
[guest@svpavliuchenv ~]$
```

Рис. 8: Проверка атрибутов директории tmp

По результатам без Sticky-бита запись в файл и дозапись в файл оказались возможной, зато удаление файла прошло неудачно, а с наоборот.

```
[guest2@svpavliuchenkov svpavliuchenkov]$ echo "test2" > /tmp/file1.txt
[guest2@svpavliuchenkov svpavliuchenkov]$ cat /tmp/file1.txt
test2
[guest2@svpavliuchenkov svpavliuchenkov]$ echo "test2" >> /tmp/file1.txt
[guest2@svpavliuchenkov svpavliuchenkov]$ cat /tmp/file1.txt
test2
test2
[guest2@svpavliuchenkov svpavliuchenkov]$ echo "test3" > /tmp/file1.txt
[guest2@svpavliuchenkov svpavliuchenkov]$ cat /tmp/file1.txt
test3
[guest2@svpavliuchenkov svpavliuchenkov]$ rm /tmp/file1.txt
rm: cannot remove '/tmp/file1.txt': Operation not permitted
[guest2@svpavliuchenkov svpavliuchenkov]$
```

Рис. 9: Операции без Sticky

Изучил механизм изменения идентификаторов, применил SetUID- и Sticky-биты. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.