

# Презентация по лабораторной работе №5

---

Коновалова Татьяна Борисовна

2 Октября 2023

РУДН, Москва, Россия

# **Презентация по лабораторной работы №5**

---

## Цель лабораторной работы №5

Цель: Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получить практические навыки работы в консоли с дополнительными атрибутами. Рассмотреть работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Задачи лабораторной работы №5

- Создать программу, выводящую uid и gid, и посмотреть на вывод после добавления SetUID и SetGID битов.
- Создать программу для чтения файлов и проверить вывод после добавления SetUID бита.
- На примере папки /tmp изучить влияние Sticky бита на запись и удаление файлов.

# **Ход выполнения лабораторной работы**

---

# Создание файла

Создала программу simpleid.c со следующим текстом



```
#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;
}
```

**Рис. 1:** Текст программы simpleid.c

## Работа с созданной программой

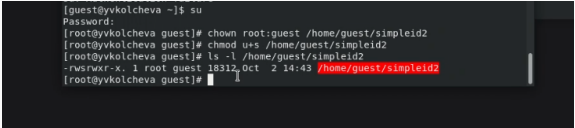
Скомпилировала программу с помощью команды gcc и убедилась, что файл действительно создан. Далее запустила исполняемый файл через ./ . Вывод написанной программы совпадает с выводом команды id

```
[guest@yvkolcheva ~]$ gcc simpleid.c -o simpleid
[guest@yvkolcheva ~]$ ./simpleid
uid=1002, gid=1002?
[guest@yvkolcheva ~]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

**Рис. 2:** Компиляция и запуск simpleid

## Установка SetUID-бит

От имени суперпользователя сменила владельца файла simpleid2 на root и установила SetUID-бит. После этого через команду `ls -l` убедилась, что бит установлен корректно



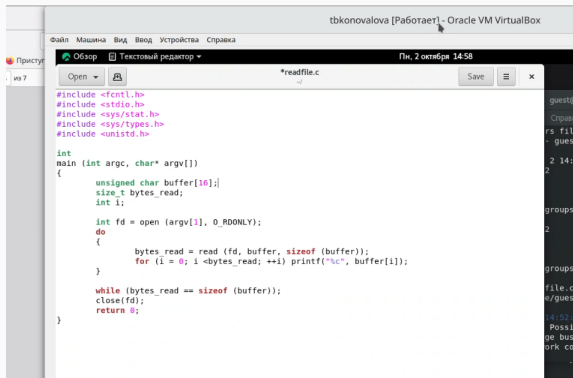
```
[guest@yvkolcheva ~]$ su
Password:
[root@yvkolcheva guest]# chown root:guest /home/guest/simpleid2
[root@yvkolcheva guest]# chmod u+s /home/guest/simpleid2
[root@yvkolcheva guest]# ls -l /home/guest/simpleid2
-rwsrwxr-x. 1 root guest 18312 Oct  2 14:43 /home/guest/simpleid2
[root@yvkolcheva guest]#
```

**Рис. 3:** Смена владельца и установка SetUID



# Работа с программой readfile.c

## Создала программу readfile.c



The screenshot shows a text editor window titled "tbkonovalova [Работает] - Oracle VM VirtualBox". The editor is displaying the source code of a C program named "readfile.c". The code includes headers for file handling, standard I/O, and system statistics. The main function takes command-line arguments and opens a file in read-only mode. It then reads the file content into a buffer and prints it character by character. The code is as follows:

```
#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[1024];
    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. 4: Текст программы readfile.c

# Наличие Sticky-бита

Проводим над файлом file01.txt следующие действия: читаем его, дозаписываем и перезаписываем информацию, переименовываем. Эти действия проходят без ошибок. При попытке удаления возникает ошибка.

```
guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test
guest2@yvkolcheva ~]$ echo "test2" >> /tmp/file01.txt
guest2@yvkolcheva ~]$ echo "test2" > /tmp/file01.txt
guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test2
guest2@yvkolcheva ~]$ echo "test3" > /tmp/file01.txt
guest2@yvkolcheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 6 Oct 2 15:19 /tmp/file01.txt
guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test3
guest2@yvkolcheva ~]$ echo "test2" > /tmp/file01.txt
guest2@yvkolcheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 6 Oct 2 15:22 /tmp/file01.txt
guest2@yvkolcheva ~]$ echo "test2" > /tmp/file01.txt
guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test2
guest2@yvkolcheva ~]$ echo "test3" > /tmp/file01.txt
guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test3
guest2@yvkolcheva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
guest2@yvkolcheva ~]$

guest2@yvkolcheva ~]$ chmod g+r /tmp/file01.txt
guest2@yvkolcheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct 2 15:09 /tmp/file01.txt
guest2@yvkolcheva ~]$ chmod g+r /tmp/file01.txt
guest2@yvkolcheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 6 Oct 2 15:19 /tmp/file01.txt
guest2@yvkolcheva ~]$
```

Рис. 5: Действия над file01.txt от лица guest2

# Изменение Sticky-бита

От имени суперпользователя удаляем sticky-бит командой `chmod -t`.

```
[root@yvvkolcheva guest]# chmod -t /tmp
[root@yvvkolcheva guest]# exit
exit
[guest@yvvkolcheva ~]$
```

**Рис. 6:** Удаление Sticky-бита

# Отсутствие Sticky-бита

Повторяем описанные ранее действия над файлом file01.txt. Теперь пользователь может удалить не принадлежащий ему файл.

```
[guest2@yvkolcheva ~]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 Oct 2 15:09 tmp
[guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test3
[guest2@yvkolcheva ~]$ echo "test2" >> /tmp/file01.txt
[guest2@yvkolcheva ~]$ cat /tmp/file01.txt
test3
test2
[guest2@yvkolcheva ~]$ rm /tmp/file01.txt
[guest2@yvkolcheva ~]$
```

Рис. 7: Повтор действий

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.

## СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>

2.Теоретические знания, приведённые в Лабораторной работе №5 -

[https://esystem.rudn.ru/pluginfile.php/2090129/mod\\_resource/content/1/lab\\_discret\\_sticky.pdf](https://esystem.rudn.ru/pluginfile.php/2090129/mod_resource/content/1/lab_discret_sticky.pdf)

## СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ:

<https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>

**Спасибо за внимание!**