

## Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Афтаева К.В.

7 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

## Информация

---

- Афтаева Ксения Васильевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201739@pfur.ru
- [https://github.com/KVAftaeva/study\\_2023-2024\\_infosec](https://github.com/KVAftaeva/study_2023-2024_infosec)

## Вводная часть

---

- Система прав доступа к файлам является одной из самых важных в операционной системе Linux

- ОС Linux
- Механизм изменения идентификаторов
- SetUID-, SetGID-, Sticky-биты

1. Подготовить лабораторный стенд, если это требуется.
2. Выполнить задания по созданию и компилированию программ.
3. Выполнить задания по исследованию Sticky-бита.

- Механизм изменения идентификаторов в ОС Linux



## Выполнение работы

---

## Исследование SetUID- и SetGID-битов

```
[guest@kvaftaeva ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] password for guest:
[guest@kvaftaeva ~]$ sudo chmod u+s /home/guest/simpleid2
[guest@kvaftaeva ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Oct  6 19:15 simpleid2
[guest@kvaftaeva ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kvaftaeva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
[guest@kvaftaeva ~]$ sudo chown root:root /home/guest/simpleid2
[sudo] password for guest:
[guest@kvaftaeva ~]$ sudo chmod g+s /home/guest/simpleid2
[guest@kvaftaeva ~]$ ls -l simpleid2
-rwxr-sr-x. 1 root root 26064 Oct  6 19:15 simpleid2
[guest@kvaftaeva ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@kvaftaeva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
```

```
[guest@kvaftaeva ~]$ chown root /home/guest/readfile
chown: changing ownership of '/home/guest/readfile': Operation not permitted
[guest@kvaftaeva ~]$ sudo chown root /home/guest/readfile
[sudo] password for guest:
[guest@kvaftaeva ~]$ chmod 733 /home/guest/readfile
chmod: changing permissions of '/home/guest/readfile': Operation not permitted
[guest@kvaftaeva ~]$ sudo chmod 733 /home/guest/readfile
[guest@kvaftaeva ~]$ ls -l readfile
-rwx-wx-wx. 1 root guest 26008 Oct  6 19:42 readfile
[guest@kvaftaeva ~]$ cat readfile
cat: readfile: Permission denied
[guest@kvaftaeva ~]$ sudo chown guest:guest /home/guest/readfile
[guest@kvaftaeva ~]$ sudo chmod u+s /home/guest/readfile
```

## Проверка возможности чтения файла

```
[guest@kvaftaeva ~]$ ./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 -- > 0);
    close (fd);
    return 0;
}
[guest@kvaftaeva ~]$
```

```
[guest@kvaftaeva ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  6 23:06 tmp
[guest@kvaftaeva ~]$ echo "test" > /tmp/file01.txt
[guest@kvaftaeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  6 23:08 /tmp/file01.txt
[guest@kvaftaeva ~]$ chmod o+rw /tmp/file01.txt
[guest@kvaftaeva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  6 23:08 /tmp/file01.txt
[guest@kvaftaeva ~]$
```

## Проверка возможных действий (со Sticky-битом)

```
[guest@kvaftaeva ~]$ su - guest2
Password:
[guest2@kvaftaeva ~]$ pwd
/home/guest2
[guest2@kvaftaeva ~]$ cd /home/guest
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@kvaftaeva guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@kvaftaeva guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@kvaftaeva guest]$
```

## Проверка возможных действий (без Sticky-бита)

```
[guest2@kvaftaeva guest]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 Oct  6 23:16 tmp
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@kvaftaeva guest]$ cat /tmp/file01.txt
test
[guest2@kvaftaeva guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@kvaftaeva guest]$ ls
```

## Результаты

---



1. Выполнены задания по созданию и компилированию программ. Изучены механизмы применения SetUID- и SetGID-битов.
2. Выполнены задания по исследованию Sticky-бита.

## Вывод

---

Я изучила механизмы изменения, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.