

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Римма Халимова НБИ-01-19

3 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

## 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 лабораторной работы**

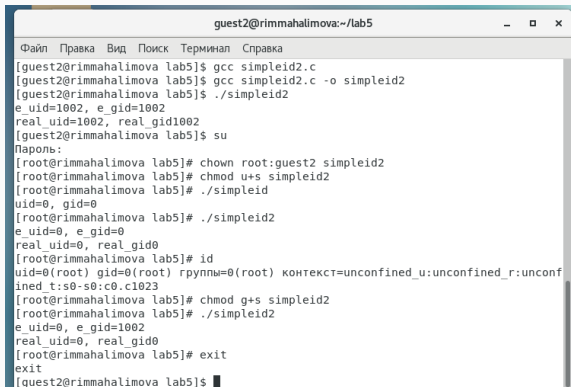
---

# Программа simpleid

```
[guest2@rimmahalimova lab5]$  
[guest2@rimmahalimova lab5]$  
[guest2@rimmahalimova lab5]$ gcc simpleid.c  
[guest2@rimmahalimova lab5]$ gcc simpleid.c -o simpleid  
[guest2@rimmahalimova lab5]$ ./simpleid  
uid=1002, gid=1002  
[guest2@rimmahalimova lab5]$ id  
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=uncon  
fined u:unconfined r:unconfined t:s0-s0:c0.c1023  
[guest2@rimmahalimova lab5]$
```

Figure 1: результат программы simpleid

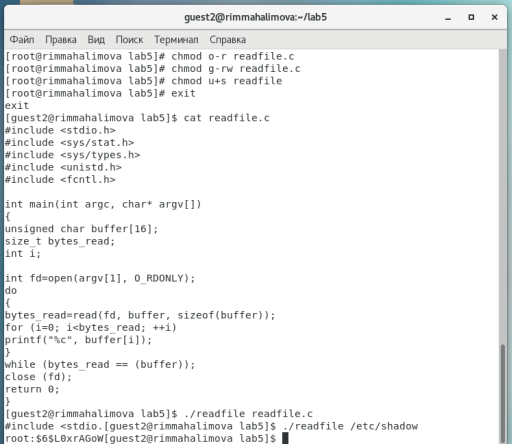
# Программа simpleid2



```
guest2@rimmahalimova:~/lab5
Файл Правка Вид Поиск Терминал Справка
[guest2@rimmahalimova lab5]$ gcc simpleid2.c
[guest2@rimmahalimova lab5]$ gcc simpleid2.c -o simpleid2
[guest2@rimmahalimova lab5]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest2@rimmahalimova lab5]$ su
Пароль:
[root@rimmahalimova lab5]# chown root:guest2 simpleid2
[root@rimmahalimova lab5]# chmod u+s simpleid2
[root@rimmahalimova lab5]# ./simpleid2
uid=0, gid=0
[root@rimmahalimova lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@rimmahalimova lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@rimmahalimova lab5]# chmod g+s simpleid2
[root@rimmahalimova lab5]# ./simpleid2
e_uid=0, e_gid=1002
real_uid=0, real_gid=0
[root@rimmahalimova lab5]# exit
exit
[guest2@rimmahalimova lab5]$
```

**Figure 2:** результат программы simpleid2

# Программа readfile



```
guest2@rimmahalimova:~/lab5
Файл Правка Вид Поиск Терминал Справка
[root@rimmahalimova lab5]# chmod o-r readfile.c
[root@rimmahalimova lab5]# chmod g-rw readfile.c
[root@rimmahalimova lab5]# chmod u+s readfile
[root@rimmahalimova lab5]# exit
exit
[guest2@rimmahalimova lab5]$ cat readfile.c
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
#include <fcntl.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 == (buffer));
    close (fd);
    return 0;
}
[guest2@rimmahalimova lab5]$ ./readfile readfile.c
#include <stdio.h>[guest2@rimmahalimova lab5]$ ./readfile /etc/shadow
root:$6$L0xrAGoW[guest2@rimmahalimova lab5]$
```

Figure 3: результат программы readfile



# Исследование Sticky-бита

```
[guest2@rimmahalimova lab5]$  
[guest2@rimmahalimova lab5]$  
[guest2@rimmahalimova lab5]$ cd /tmp/  
[guest2@rimmahalimova tmp]$ echo "test" >> file01.txt  
[guest2@rimmahalimova tmp]$ chmod o+rx file01.txt  
[guest2@rimmahalimova tmp]$ ls -l file01.txt  
-rw-rw-r-x. 1 guest2 guest2 5 окт  3 14:31 file01.txt  
[guest2@rimmahalimova tmp]$ su guest3  
Пароль:  
[guest3@rimmahalimova tmp]$ cat file01.txt  
test  
[guest3@rimmahalimova tmp]$ echo "test2" >> file01.txt  
bash: file01.txt: Отказано в доступе  
[guest3@rimmahalimova tmp]$ echo "test2" > file01.txt  
bash: file01.txt: Отказано в доступе  
[guest3@rimmahalimova tmp]$ rm file01.txt  
rm: удалить защищенный от записи обычный файл «file01.txt»? y  
rm: невозможно удалить «file01.txt»: Операция не позволена  
[guest3@rimmahalimova tmp]$ su  
Пароль:  
[root@rimmahalimova tmp]# chmod -t /tmp  
[root@rimmahalimova tmp]# exit  
exit  
[guest3@rimmahalimova tmp]$ echo "test2" >> file01.txt  
bash: file01.txt: Отказано в доступе  
[guest3@rimmahalimova tmp]$ rm file01.txt  
rm: удалить защищенный от записи обычный файл «file01.txt»? y  
[guest3@rimmahalimova tmp]$ su  
Пароль:  
[root@rimmahalimova tmp]# chmod +t /tmp  
[root@rimmahalimova tmp]#
```

Figure 4: исследование Sticky-бита

## **Выводы**

---

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.