

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Стаменкович Огнен

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

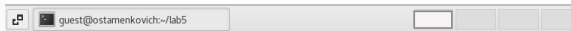
Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# **Выполнение лабораторной работы**

---

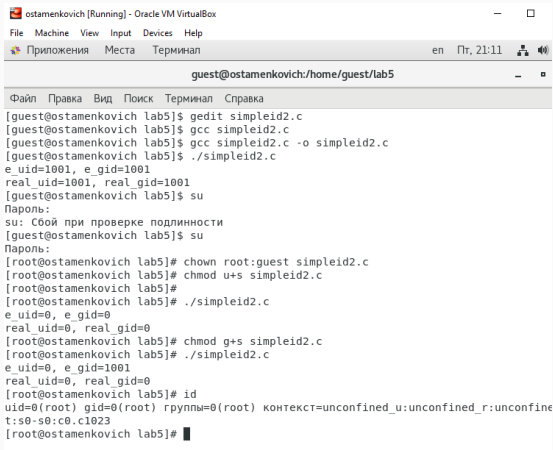
# Программа simpleid

```
[guest@ostamenkovich ~]$ cd lab5/  
[guest@ostamenkovich lab5]$ touch simpleid.c  
[guest@ostamenkovich lab5]$ touch simpleid2.c  
[guest@ostamenkovich lab5]$ touch readfile.c  
[guest@ostamenkovich lab5]$ gedit  
[guest@ostamenkovich lab5]$ gedit simpleid.c  
[guest@ostamenkovich lab5]$  
[guest@ostamenkovich lab5]$ gcc simpleid.c  
[guest@ostamenkovich lab5]$ gcc simpleid.c -o simpleid  
[guest@ostamenkovich lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@ostamenkovich lab5]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r  
:unconfined_t:s0-s0:c0.c1023  
[guest@ostamenkovich lab5]$ █
```



**Figure 1:** результат программы simpleid

# Программа simpleid2



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en Пт, 21:11
guest@ostamenkovich:/home/guest/lab5
Файл Правка Вид Поиск Терминал Справка
[guest@ostamenkovich lab5]$ gedit simpleid2.c
[guest@ostamenkovich lab5]$ gcc simpleid2.c
[guest@ostamenkovich lab5]$ gcc simpleid2.c -o simpleid2.c
[guest@ostamenkovich lab5]$ ./simpleid2.c
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@ostamenkovich lab5]$ su
Пароль:
su: Сбой при проверке подлинности
[guest@ostamenkovich lab5]$ su
Пароль:
[root@ostamenkovich lab5]# chown root:guest simpleid2.c
[root@ostamenkovich lab5]# chmod u+s simpleid2.c
[root@ostamenkovich lab5]#
[root@ostamenkovich lab5]# ./simpleid2.c
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@ostamenkovich lab5]# chmod g+s simpleid2.c
[root@ostamenkovich lab5]# ./simpleid2.c
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@ostamenkovich lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfine
t:s0-s0:c0.c1023
[root@ostamenkovich lab5]#
```

Figure 2: результат программы simpleid2

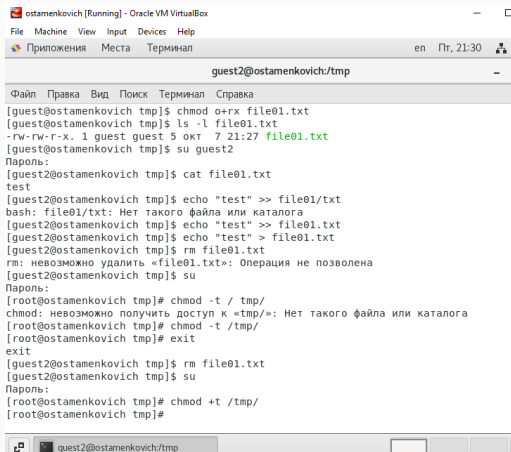
# Программа readfile

```
(gedit:5639): dconf-WARNING **: 21:23:54.359: failed to commit changes to dconf
инение закрыто
[root@ostamenkovich guest]# gcc readfile.c
[root@ostamenkovich guest]# gcc readfile.c -o readfile
[root@ostamenkovich guest]# chown root:root readfile
[root@ostamenkovich guest]# chmod -r readfile.c
[root@ostamenkovich guest]# chmod u+s readfile
[root@ostamenkovich guest]# exit
exit
[guest@ostamenkovich ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@ostamenkovich ~]$ ./readfile readfile.c
```

**Figure 3:** результат программы readfile



# Исследование Sticky-бита



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en Пт, 21:30
guest2@ostamenkovich:/tmp

Файл Правка Вид Поиск Терминал Справка
[guest@ostamenkovich tmp]$ chmod o+rx file01.txt
[guest@ostamenkovich tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 guest guest 5 окт  7 21:27 file01.txt
[guest@ostamenkovich tmp]$ su guest2
Пароль:
[guest2@ostamenkovich tmp]$ cat file01.txt
test
[guest2@ostamenkovich tmp]$ echo "test" >> file01/txt
bash: file01/txt: Нет такого файла или каталога
[guest2@ostamenkovich tmp]$ echo "test" >> file01.txt
[guest2@ostamenkovich tmp]$ echo "test" > file01.txt
[guest2@ostamenkovich tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@ostamenkovich tmp]$ su
Пароль:
[root@ostamenkovich tmp]# chmod -t /tmp/
chmod: невозможно получить доступ к «tmp/»: Нет такого файла или каталога
[root@ostamenkovich tmp]# chmod -t /tmp/
[root@ostamenkovich tmp]# exit
exit
[guest2@ostamenkovich tmp]$ rm file01.txt
[guest2@ostamenkovich tmp]$ su
Пароль:
[root@ostamenkovich tmp]# chmod +t /tmp/
[root@ostamenkovich 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.