

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Миша Нкого Хосе Адольфо Мба НФИбд-02-19

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

```
[guest@mnkongo lab5]$ touch readfile.c
[guest@mnkongo lab5]$ gedit simpleid.c
[guest@mnkongo lab5]$
[guest@mnkongo lab5]$ gcc simpleid.c
[guest@mnkongo lab5]$ gcc simpleid.c -o simpleid
[guest@mnkongo lab5]$ ./simpleid
uid=1001, gid=1001
[guest@mnkongo lab5]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[guest@mnkongo lab5]$
```

Figure 1: результат программы simpleid

# Программа simpleid2

```
[guest@mnkongo lab5]$  
[guest@mnkongo lab5]$ gcc simpleid2.c  
[guest@mnkongo lab5]$ gcc simpleid2.c -o simpleid2.c  
[guest@mnkongo lab5]$ ./simpleid2  
bash: ./simpleid2: Нет такого файла или каталога  
[guest@mnkongo lab5]$ ./simpleid2.c  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@mnkongo lab5]$ su  
Пароль:  
[root@mnkongo lab5]# chown root:guest simpleid2.c  
[root@mnkongo lab5]# chmod u+s simpleid2.c  
[root@mnkongo lab5]# id  
uid=0(root) gid=0(root) rгруппы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@mnkongo lab5]# ./simpleid2.c  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@mnkongo lab5]# chmod g+s simpleid2.c  
[root@mnkongo lab5]# ./simpleid2.c  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=0  
[root@mnkongo lab5]# exit  
exit  
[guest@mnkongo lab5]$
```

**Figure 2:** результат программы simpleid2

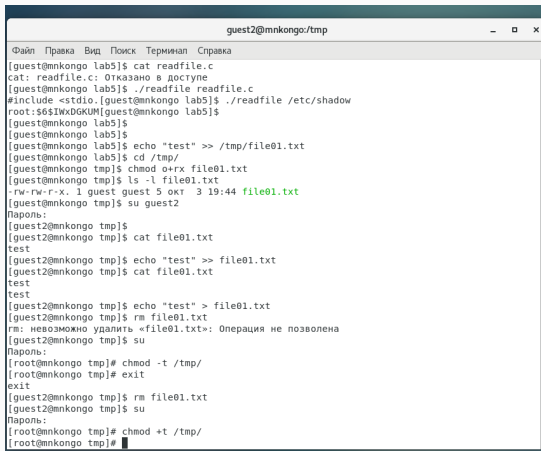
# Программа readfile

```
exit
[guest@mnkongo lab5]$ gedit readfile.c
[guest@mnkongo lab5]$
[guest@mnkongo lab5]$
[guest@mnkongo lab5]$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
while (bytes_read == (buffer));
                    ^
[guest@mnkongo lab5]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
while (bytes_read == (buffer));
                    ^
[guest@mnkongo lab5]$ su
Пароль:
[root@mnkongo lab5]# chown root:root readfile
[root@mnkongo lab5]# chmod -r readfile.c
[root@mnkongo lab5]# chmod u+s readfile
[root@mnkongo lab5]# ls -l readfile.c
--w--w----. 1 guest guest 386 окр  3 19:43 readfile.c
[root@mnkongo lab5]# exit
exit
[guest@mnkongo lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@mnkongo lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@mnkongo lab5]$ ./readfile /etc/shadow
root:$6$IWxDGKUM[guest@mnkongo lab5]$
```

Figure 3: результат программы readfile



# Исследование Sticky-бита



```
guest2@mnkongo:/tmp
Файл Правка Вид Поиск Терминал Справка
[guest@mnkongo lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@mnkongo lab5]$ ./readfile readfile.c
#include <stdio.h>
[guest@mnkongo lab5]$ ./readfile /etc/shadow
root:$6$IWxDGKUM[guest@mnkongo lab5]$
[guest@mnkongo lab5]$
[guest@mnkongo lab5]$
[guest@mnkongo lab5]$ echo "test" >> /tmp/file01.txt
[guest@mnkongo lab5]$ cd /tmp/
[guest@mnkongo tmp]$ chmod o+rx file01.txt
[guest@mnkongo tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 guest guest 5 окр  3 19:44 file01.txt
[guest@mnkongo tmp]$ su guest2
Пароль:
[guest2@mnkongo tmp]$
[guest2@mnkongo tmp]$ cat file01.txt
test
[guest2@mnkongo tmp]$ echo "test" >> file01.txt
[guest2@mnkongo tmp]$ cat file01.txt
test
test
[guest2@mnkongo tmp]$ echo "test" > file01.txt
[guest2@mnkongo tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@mnkongo tmp]$ su
Пароль:
[root@mnkongo tmp]# chmod -t /tmp/
[root@mnkongo tmp]# exit
exit
[guest2@mnkongo tmp]$ rm file01.txt
[guest2@mnkongo tmp]$ su
Пароль:
[root@mnkongo tmp]# chmod +t /tmp/
[root@mnkongo 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.