

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Кирилл Дроздков НПИбд-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.

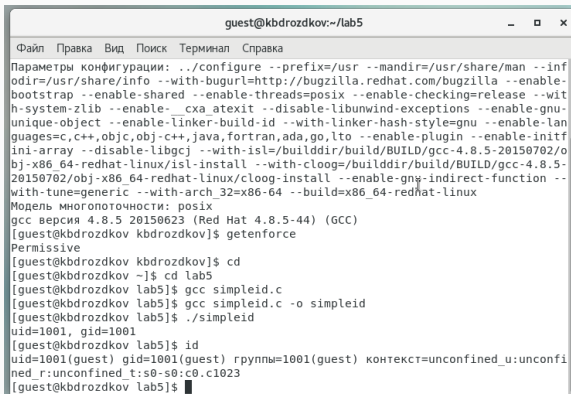
## Цель лабораторной работы

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**

---

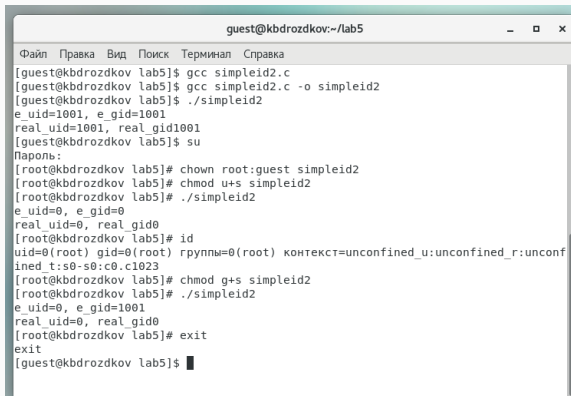
# Программа simpleid

A terminal window titled 'guest@kbrozdokov:~/lab5' with standard window controls. The terminal shows the output of the 'simpleid' program, which displays configuration parameters, the multi-threading model (posix), GCC version (4.8.5), and the user's permissions (uid=1001, gid=1001, rpyнны=1001, context=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023).

```
guest@kbrozdokov:~/lab5
Файл  Правка  Вид  Поиск  Терминал  Справка
Параметры конфигурации: ../configure --prefix=/usr --mandir=/usr/share/man --inf
odir=/usr/share/info --with-bugurl=http://bugzilla.redhat.com/bugzilla --enable-
bootstrap --enable-shared --enable-threads=posix --enable-checking=release --wit
h-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-
unique-object --enable-linker-build-id --with-linker-hash-style=gnu --enable-lan
guages=c,c++,objc,obj-c++,java,fortran,ada,go,lto --enable-plugin --enable-initf
ini-array --disable-libgck --with-isl=/builddir/build/BUILD/gcc-4.8.5-20150702/o
bj-x86_64-redhat-linux/isl-install --with-cloog=/builddir/build/BUILD/gcc-4.8.5-
20150702/obj-x86_64-redhat-linux/cloog-install --enable-gn-indirect-function --
with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Модель многопоточности: posix
gcc версия 4.8.5 20150623 (Red Hat 4.8.5-44) (GCC)
[guest@kbrozdokov kbrozdokov]$ getenforce
Permissive
[guest@kbrozdokov kbrozdokov]$ cd
[guest@kbrozdokov ~]$ cd lab5
[guest@kbrozdokov lab5]$ gcc simpleid.c
[guest@kbrozdokov lab5]$ gcc simpleid.c -o simpleid
[guest@kbrozdokov lab5]$ ./simpleid
uid=1001, gid=1001
[guest@kbrozdokov lab5]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@kbrozdokov lab5]$
```

Figure 1: результат программы simpleid

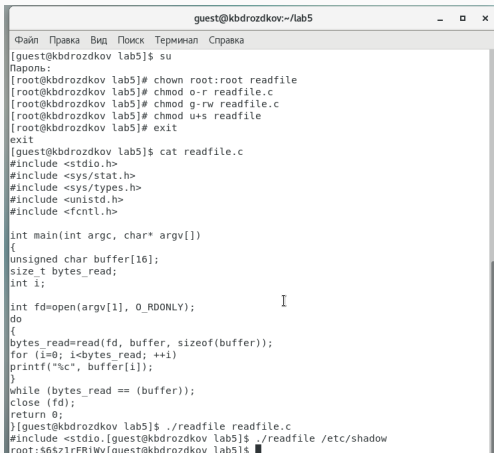
# Программа simpleid2



```
guest@kbrozdkov:~/lab5
Файл Правка Вид Поиск Терминал Справка
[guest@kbrozdkov lab5]$ gcc simpleid2.c
[guest@kbrozdkov lab5]$ gcc simpleid2.c -o simpleid2
[guest@kbrozdkov lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kbrozdkov lab5]$ su
Пароль:
[root@kbrozdkov lab5]# chown root:guest simpleid2
[root@kbrozdkov lab5]# chmod u+s simpleid2
[root@kbrozdkov lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@kbrozdkov lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@kbrozdkov lab5]# chmod g+s simpleid2
[root@kbrozdkov lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@kbrozdkov lab5]# exit
exit
[guest@kbrozdkov lab5]$
```

**Figure 2:** результат программы simpleid2

# Программа readfile



```
guest@kbrozdtkov:~/lab5
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@kbrozdtkov lab5]$ su
Пароль:
[root@kbrozdtkov lab5]# chown root:root readfile
[root@kbrozdtkov lab5]# chmod o-r readfile.c
[root@kbrozdtkov lab5]# chmod g-rw readfile.c
[root@kbrozdtkov lab5]# chmod u+s readfile
[root@kbrozdtkov lab5]# exit
exit
[guest@kbrozdtkov lab5]$ cat readfile.c
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
#include <fcntl.h>

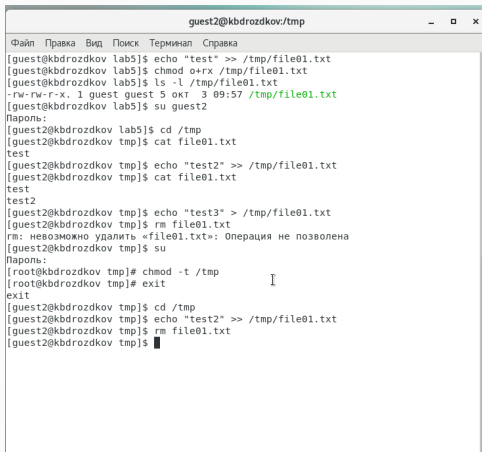
int main(int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    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;
}
[guest@kbrozdtkov lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@kbrozdtkov lab5]$ ./readfile /etc/shadow
root:$6$2lrFRiWy[guest@kbrozdtkov lab5]$
```

**Figure 3:** результат программы readfile



# Исследование Sticky-бита



```
guest2@kbrozdKov:tmp
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@kbrozdKov lab5]$ echo "test" >> /tmp/file01.txt
[guest@kbrozdKov lab5]$ chmod o+rx /tmp/file01.txt
[guest@kbrozdKov lab5]$ ls -l /tmp/file01.txt
-rw-rw-r-x. 1 guest guest 5 окт  3 09:57 /tmp/file01.txt
[guest@kbrozdKov lab5]$ su guest2
Пароль:
[guest2@kbrozdKov lab5]$ cd /tmp
[guest2@kbrozdKov tmp]$ cat file01.txt
test
[guest2@kbrozdKov tmp]$ echo "test2" >> /tmp/file01.txt
[guest2@kbrozdKov tmp]$ cat file01.txt
test
test2
[guest2@kbrozdKov tmp]$ echo "test3" > /tmp/file01.txt
[guest2@kbrozdKov tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@kbrozdKov tmp]$ su
Пароль:
[root@kbrozdKov tmp]# chmod -t /tmp
[root@kbrozdKov tmp]# exit
exit
[guest2@kbrozdKov tmp]$ cd /tmp
[guest2@kbrozdKov tmp]$ echo "test2" >> /tmp/file01.txt
[guest2@kbrozdKov tmp]$ rm file01.txt
[guest2@kbrozdKov 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.