

# Лабораторная работа №5

## Основы информационной безопасности

---

Белов Н.Д.

02 октября 2022

Российский университет дружбы народов, Москва, Россия

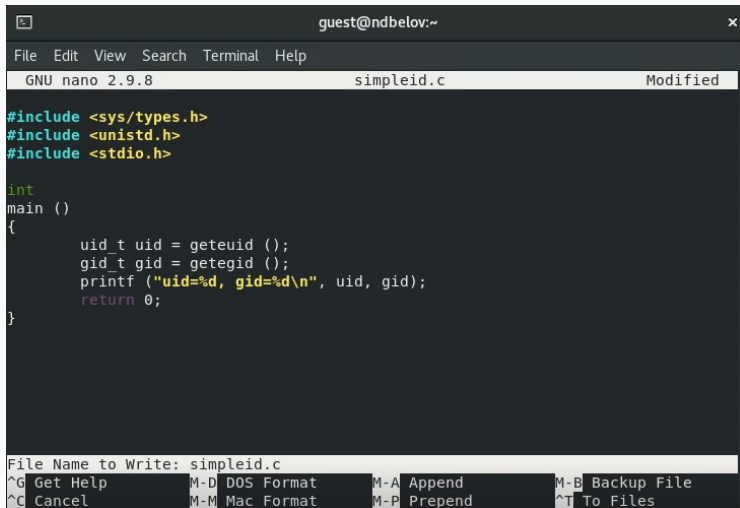
## Исследование влияния дополнительных атрибутов

---

## Цель выполнения лабораторной работы

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

- Написал программу simpleid от имени пользователя guest



```
guest@ndbelov:~  
File Edit View Search Terminal Help  
GNU nano 2.9.8 simpleid.c Modified  
  
#include <sys/types.h>  
#include <unistd.h>  
#include <stdio.h>  
  
int  
main ()  
{  
    uid_t uid = geteuid ();  
    gid_t gid = getegid ();  
    printf ("uid=%d, gid=%d\n", uid, gid);  
    return 0;  
}  
  
File Name to Write: simpleid.c  
^G Get Help      M-D DOS Format  M-A Append      M-B Backup File  
^C Cancel        M-M Mac Format  M-P Prepend     ^T To Files
```

- Выполнил программу `id` и сравнил полученный результат с данными программы

```
[guest@ndbelov ~]$ nano simpleid.c
[guest@ndbelov ~]$ gcc simpleid.c -o simpleid
[guest@ndbelov ~]$ ./simpleid
uid=1001, gid=1001
[guest@ndbelov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 2: Сравнение результатов программы и команды

- Усложнил программу, добавив вывод действительных идентификаторов

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t real_uid = getuid ();
    uid_t e_uid = geteuid ();

    gid_t real_gid = getgid ();
    gid_t e_gid = getegid ();

    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);

    return 0;
}
```

File Name to Write: simpleid2.c

^G Get Help	M-D DOS Format	M-A Append	M-B Backup File
^C Cancel	M-M Mac Format	M-P Prepend	^T To Files

Figure 3: Код программы simpleid2.c

- Скомпилировал и запустил simpleid2.c `gcc simpleid2.c -o simpleid2`

```
[guest@ndbelov ~]$ gcc simpleid2.c -o simpleid2
[guest@ndbelov ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Figure 4: Компиляция и запуск simpleid2.c

- Сменил у программы readfile владельца и установил SetU'D-бит

```
[guest@ndbelov ~]$ ls -l / | grep tmp
drwxrwxrwt. 13 root root 4096 Oct  2 18:09 tmp
[guest@ndbelov ~]$ echo "test" > /tmp/file01.txt
[guest@ndbelov ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  2 18:10 /tmp/file01.txt
[guest@ndbelov ~]$ chmod o+rw /tmp/file01.txt
[guest@ndbelov ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  2 18:10 /tmp/file01.txt
```

Figure 5: Проверка атрибутов



- Проверка выполнения операций от пользователя guest2

```
[guest@ndbelov ~]$ su guest2
Password:
[guest2@ndbelov guest]$ cat /tmp/file01.txt
test
[guest2@ndbelov guest]$ echo "test" > /tmp/file01.txt
[guest2@ndbelov guest]$ echo "test2" > /tmp/file01.txt
[guest2@ndbelov guest]$ cat /tmp/file01.txt
test2
[guest2@ndbelov guest]$ echo "test3" > /tmp/file01.txt
[guest2@ndbelov guest]$ cat /tmp/file01.txt
test3
[guest2@ndbelov guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Figure 6: Проверка от guest2

- Снял атрибут `t` с директории `/tmp` и повторил операции

```
[guest2@ndbelov guest]$ su -  
Password:  
[root@ndbelov ~]# chmod -t /tmp  
[root@ndbelov ~]# exit  
logout  
[guest2@ndbelov guest]$ ls -l / | grep tmp  
drwxrwxrwx. 13 root root 4096 Oct  2 18:14 tmp  
[guest2@ndbelov guest]$ su -  
Password:  
[root@ndbelov ~]# chmod +t /tmp  
[root@ndbelov ~]# exit  
logout  
[guest2@ndbelov guest]$ ls -l / | grep tmp  
drwxrwxrwt. 14 root root 4096 Oct  2 18:15 tmp
```

Figure 7: Проверка после снятия Sticky атрибута

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