

ЛАБОРАТОРНАЯ РАБОТА №5

Доре Стевенсон Эдгар - СТУДЕНТ ГРУППЫ НКНБД-01-19

08.10.2022

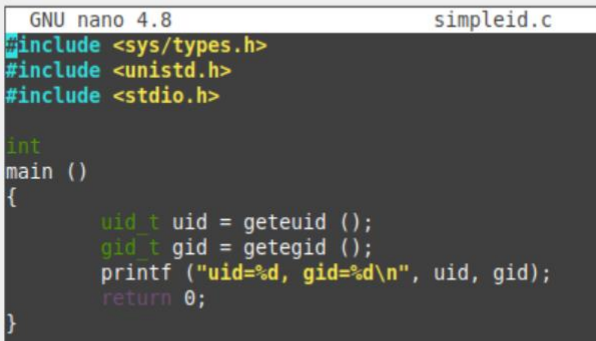
ИССЛЕДОВАНИЕ ВЛИЯНИЯ ДОПОЛ-НИТЕЛЬНЫХ АТТРИБУТОВ

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.

ВЫПОЛНЕНИЕ

- Написал программу simpleid от имени пользователя guest



```
GNU nano 4.8 simpleid.c
#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;
}
```

Рис. 1: Код программы 'simpleid.c'

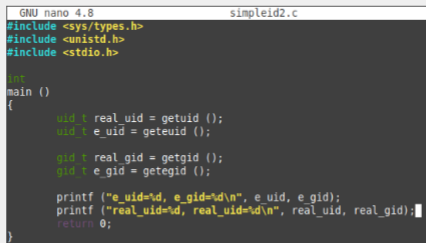
- Выполнил программу `id` и сравнил полученный результат с данными программы

```
$ nano simpleid.c
$ gcc simpleid.c -o simpleid
$ ./simpleid
uid=1001, gid=1001
$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest)
$
```

Рис. 2: Сравнение результатов программы и команды

ВЫПОЛНЕНИЕ

- Усложнил программу, добавив вывод действительных идентификаторов



```
GNU nano 4.8 simpleid2.c
#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;
}
```

Рис. 3: Код программы simpleid2.c

ВЫПОЛНЕНИЕ

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

```
$ nano simpleid2.c
$ gcc simpleid2.c -o simpleid2
$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 4: Компиляция и запуск simpleid2.c

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

```
$ ls -l / | grep tmp
drwxrwxrwt 15 root root      4096 ноя 13 18:54 tmp
$ echo "test" > /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-r-- 1 guest guest 5 ноя 13 19:03 /tmp/file01.txt
$ chmod o+rw /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-rw- 1 guest guest 5 ноя 13 19:03 /tmp/file01.txt
$
```

Рис. 5: Проверка атрибутов

■ Проверка выполнения операций от пользователя guest2

```
mint@mint-VirtualBox:~/Рабочий стол$ su - guest2
Пароль:
$ cat /tmp/file01.txt
test
$ echo "test2" > /tmp/file01.txt
-sh: 2: cannot create /tmp/file01.txt: Permission denied
$ echo "test3" > /tmp/file01.tx
$ echo "test3" > /tmp/file01.txt
-sh: 4: cannot create /tmp/file01.txt: Permission denied
$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
$ su -
```

Рис. 6: Проверка от guest2

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

```
$ ls -l / | grep tmp
drwxrwxrwx 15 root root      4096 ноя 13 19:07 tmp
$ echo "test2" > /tmp/file01.txt
$ cat /tmp/file01.txt
test2
$ rm /tmp/file01.txt
$
```

Рис. 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.