

Лабораторная работа №5

Дискреционное разграничение прав в Linux.

Исследование влияния дополнительных атрибутов.

Лилия М. Пономарёва НПИбд-02-19¹

2022, 19 March, Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

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.

Создала программу simpleid.c

```
GNU nano 5.6.1                                     simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t uid = getuid ();
    gid_t gid = getgid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Рис. 1: Код программы simpleid.c

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

Рис. 2: Компиляция и выполнение программы

```
GNU nano 5.6.1                                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: Программа simpleid2.c

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

Рис. 4: Вывод реальных и действительных идентификаторов

Смена владельца и группы файла simpleid2 и его прав доступа

```
[guest@lmponomareva ~]$ su  
Password:  
[root@lmponomareva guest]# chown root:guest /home/guest/simpleid2  
[root@lmponomareva guest]# chmod u+s /home/guest/simpleid2
```

Рис. 5: Смена владельца файла и прав доступа

```
[guest@lmponomareva ~]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  8 11:36 simpleid2
[guest@lmponomareva ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@lmponomareva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 6: Вывод программы simpleid2

Проделали тоже самое относительно SetGID-бита

```
[guest@lmponomareva ~]$ su -  
Password:  
[root@lmponomareva ~]# chown root:root /home/guest/simpleid2  
[root@lmponomareva ~]# chmod g+s /home/guest/simpleid2  
[root@lmponomareva ~]# su guest  
[guest@lmponomareva root]$ cd /home/guest  
[guest@lmponomareva ~]$ ls -l  
total 96  
drwx-----. 3 guest guest   31 Oct  1 12:01 dir1  
-rwsrwxr-x. 1 root  guest 25952 Oct  8 11:47 readfile  
-r------. 1 root  guest   416 Oct  8 11:47 readfile.c  
-rwxrwxr-x. 1 guest guest 25904 Oct  8 11:30 simpleid  
-rwxrwsr-x. 1 root  root  26008 Oct  8 11:36 simpleid2  
-rw-rw-r--. 1 guest guest   310 Oct  8 11:35 simpleid2.c  
-rw-rw-r--. 1 guest guest   177 Oct  8 11:30 simpleid.c  
[guest@lmponomareva ~]$ ./simpleid2  
e_uid=1001, e_gid=0  
real_uid=1001, real_gid=1001
```

Рис. 7: SetGID-бит

```
GNU nano 5.6.1                                readfile.c

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 == sizeof (buffer));
    close (fd);
    return 0;
}
```

Рис. 8: Код программы readfile.c

```
[guest@lmponomareva ~]$ gcc readfile.c -o readfile  
[guest@lmponomareva ~]$
```

Рис. 9: Компиляция

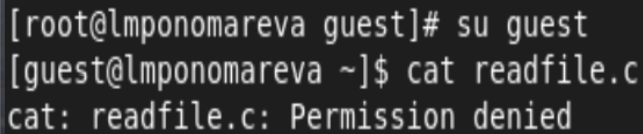
Смена владельца файла readfile.c

```
[root@lmponomareva guest]# chown root readfile.c
[root@lmponomareva guest]# ls -l
total 96
drwx-----. 3 guest guest    31 Oct  1 12:01 dir1
-rwxrwxr-x. 1 guest guest 25952 Oct  8 11:47 readfile
-rw-rw-r--. 1 root  guest   416 Oct  8 11:47 readfile.c
```

Рис. 10: Смена владельца файла

```
[root@lmponomareva guest]# chmod 000 readfile.c
[root@lmponomareva guest]# ls -l
total 96
drwx-----. 3 guest guest    31 Oct  1 12:01 dir1
-rwxrwxr-x. 1 guest guest 25952 Oct  8 11:47 readfile
-----. 1 root guest    416 Oct  8 11:47 readfile.c
-rwxrwxr-x. 1 guest guest 25904 Oct  8 11:30 simpleid
-rwsrwxr-x. 1 root guest 26008 Oct  8 11:36 simpleid2
-rw-rw-r--. 1 guest guest   310 Oct  8 11:35 simpleid2.c
-rw-rw-r--. 1 guest guest   177 Oct  8 11:30 simpleid.c
[root@lmponomareva guest]# chmod u+r readfile.c
[root@lmponomareva guest]# ls -l
total 96
drwx-----. 3 guest guest    31 Oct  1 12:01 dir1
-rwxrwxr-x. 1 guest guest 25952 Oct  8 11:47 readfile
-r-----. 1 root guest    416 Oct  8 11:47 readfile.c
```

Рис. 11: Смена атрибутов

A terminal window with a black background and white text. The text shows a root user switching to a guest user and then attempting to run the 'cat' command on a file named 'readfile.c'. The command fails with a 'Permission denied' error.

```
[root@lmponomareva guest]# su guest  
[guest@lmponomareva ~]$ cat readfile.c  
cat: readfile.c: Permission denied
```

Рис. 12: Проверка доступа к файлу

Смена владельца и установка SetUID-бит

```
[root@lmponomareva guest]# chown root readfile
[root@lmponomareva guest]# ls -l
total 96
drwx----- . 3 guest guest    31 Oct  1 12:01 dir1
-rwxrwxr-x. 1 root  guest 25952 Oct  8 11:47 readfile
-r----- . 1 root  guest   416 Oct  8 11:47 readfile.c
-rwxrwxr-x. 1 guest guest 25904 Oct  8 11:30 simpleid
-rwsrwxr-x. 1 root  guest 26008 Oct  8 11:36 simpleid2
-rw-rw-r-- . 1 guest guest   310 Oct  8 11:35 simpleid2.c
-rw-rw-r-- . 1 guest guest   177 Oct  8 11:30 simpleid.c
[root@lmponomareva guest]# chmod u+s readfile
[root@lmponomareva guest]# ls -l
total 96
drwx----- . 3 guest guest    31 Oct  1 12:01 dir1
-rwsrwxr-x. 1 root  guest 25952 Oct  8 11:47 readfile
```

Рис. 13: Смена владельца и добавление SetUID у readfile

Выполнение программы readfile

```
[guest@lmponomareva ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.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]);
    }
}
```

Рис. 14: Чтение файла readfile.c программой readfile

Чтение файла /etc/shadow

```
[guest@lmponomareva ~]$ ./readfile /etc/shadow
root:$6$W2IR6nS3QWKTikL2$r4H9pvGoJtHwSwGVHYR/Wv
zjuvHIne08CntHHPH8dqCK1q/::0:99999:7:::
bin:*:19123:0:99999:7:::
daemon:*:19123:0:99999:7:::
adm:*:19123:0:99999:7:::
lp:*:19123:0:99999:7:::
sync:*:19123:0:99999:7:::
shutdown:*:19123:0:99999:7:::
halt:*:19123:0:99999:7:::
mail:*:19123:0:99999:7:::
operator:*:19123:0:99999:7:::
games:*:19123:0:99999:7:::
```

Рис. 15: Чтение файла /etc/shadow программой из readfile

Наличие атрибута Sticky на директории /tmp

```
[guest@lmponomareva ~]$ ls -l / | grep tmp  
drwxrwxrwt. 17 root root 4096 Oct  8 21:13 tmp  
[guest@lmponomareva ~]$
```

Рис. 16: Атрибут Sticky на директории /tmp

Создали файл file01.txt в директории /tmp со словом test

```
[guest@lmponomareva ~]$ echo "test" > /tmp/file01.txt  
[guest@lmponomareva ~]$
```

Рис. 17: Создание файла file01.txt в директории /tmp

Чтение и запись для категории пользователей «все остальные»

```
[guest@lmponomareva ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 21:14 /tmp/file01.txt
[guest@lmponomareva ~]$ chmod o+w /tmp/file01.txt
[guest@lmponomareva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 21:14 /tmp/file01.txt
```

Рис. 18: Чтение и запись для категории пользователей «все остальные»

От пользователя guest2 прочитали файл /tmp/file01.txt

```
[guest@lmponomareva ~]$ su guest2  
Password:  
[guest2@lmponomareva guest]$ cat /tmp/file01.txt  
test
```

Рис. 19: Чтение файла /tmp/file01.txt

От пользователя guest2 дозаписали файл /tmp/file01.txt

```
[guest2@lmponomareva guest]$ echo "test2" >> /tmp/file01.txt  
[guest2@lmponomareva guest]$ cat /tmp/file01.txt  
test  
test2
```

Рис. 20: Дозапись файла /tmp/file01.txt

От пользователя guest2 перезапись файла /tmp/file01.txt

```
[guest2@lmponomareva guest]$ echo "test3" > /tmp/file01.txt  
[guest2@lmponomareva guest]$ cat /tmp/file01.txt  
test3
```

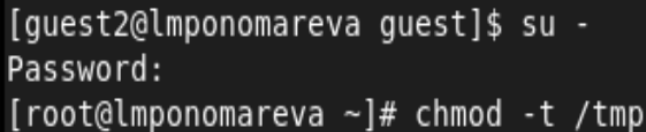
Рис. 21: Перезапись файла /tmp/file01.txt

Попытка удалить файл /tmp/file01.txt

```
[guest2@lmponomareva guest]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': Operation not permitted  
[guest2@lmponomareva guest]$ █
```

Рис. 22: Попытка удаления файла /tmp/file01.txt

Сняли атрибут t (Sticky-бит) с директории /tmp

A terminal window with a dark background and light gray text. The prompt is [guest2@lmponomareva guest]\$. The user enters 'su -'. The prompt changes to [root@lmponomareva ~]#. The user enters 'chmod -t /tmp'.

```
[guest2@lmponomareva guest]$ su -  
Password:  
[root@lmponomareva ~]# chmod -t /tmp
```

Рис. 23: Снятие Sticky-бит

От пользователя guest2 проверили, что атрибута t у директории /tmp

нет

```
[root@lmponomareva ~]# exit
logout
[guest2@lmponomareva guest]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  8 21:19 tmp
```

Рис. 24: Проверка атрибутов

Повторили предыдущие шаги

```
[guest2@lmponomareva guest]$ cat /tmp/file01.txt  
test3  
[guest2@lmponomareva guest]$ echo "test4" > /tmp/file01.txt  
[guest2@lmponomareva guest]$ cat /tmp/file01.txt  
test4  
[guest2@lmponomareva guest]$ rm /tmp/file01.txt  
[guest2@lmponomareva guest]$
```

Рис. 25: Проверка атрибутов

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.