Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Липатникова Марина Сергеевна

08.10.2022, Moscow

RUDN University, Moscow, Russian Federation

Цель 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

```
[guest@mslipatnikova ~]$ touch simpleid.c
[guest@mslipatnikova ~]$ nano simpleid.c
[guest@mslipatnikova ~]$ cat 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;
}
[guest@mslipatnikova ~]$ gcc simpleid.c -o simpleid
[guest@mslipatnikova ~]$ ./simpleid
uid=1001, gid=1001
[guest@mslipatnikova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

Figure 1: Работа с программой simpleid

Выполнение лабораторной работы

```
[guest@mslipatnikova ~]$ nano simpleid.c
[guest@mslipatnikova ~]$ ls
Desktop  Documents  Music     Public    simpleid2.c  Templates
dir1     Downloads  Pictures  simpleid  simpleid.c   Videos
[guest@mslipatnikova ~]$ cat 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 ("uid=%d, gid=%d\n",e_uid,e_gid);
        printf ("real_uid=%d,real_gid=%d\n", real_uid, real_gid);
        return 0;
}
[guest@mslipatnikova ~]$ gcc simpleid2.c -o simpleid2
[guest@mslipatnikova ~]$ ./simpleid2
uid=1001, gid=1001
real_uid=1001,real_gid=1001
```

Figure 2: Работа с программой simpleid2

Выполнение лабораторной работы

Figure 3: Работа simpleid2(u+s)

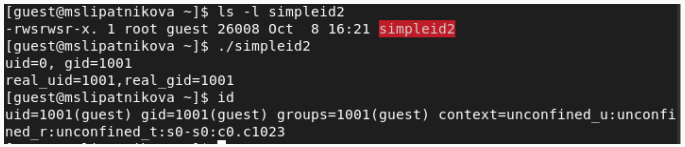


Figure 4: Работа simpleid2(g+s)

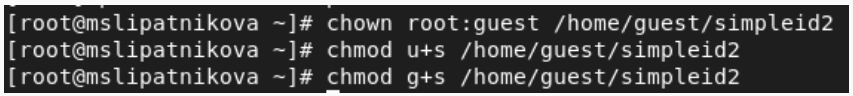
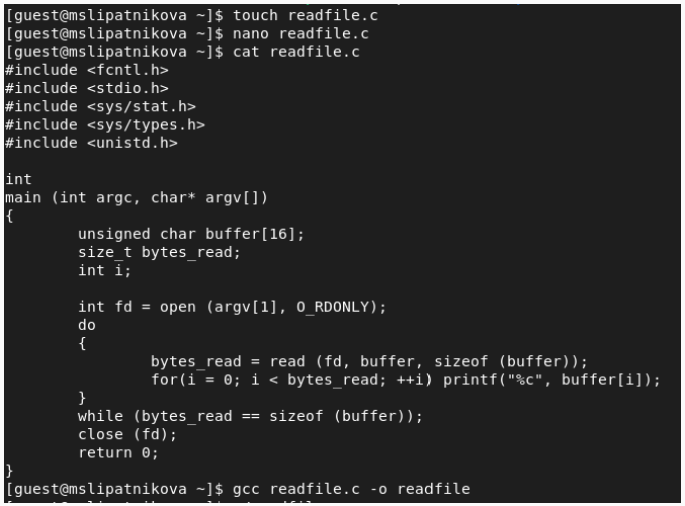


Figure 5: Команды от суперпользователя

Выполнение лабораторной работы



```
[guest@mslipatnikova ~]$ touch readfile.c
[guest@mslipatnikova ~]$ nano readfile.c
[guest@mslipatnikova ~]$ cat 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]);
        }
        while (bytes_read == sizeof (buffer));
        close (fd);
        return 0;
}
[guest@mslipatnikova ~]$ gcc readfile.c -o readfile
```

Figure 6: Программа readfile

Выполнение лабораторной работы

```
[guest@mslipatnikova ~]$ ls -l readfile.c
-rwx------. 1 root guest 418 Oct  8 17:10 readfile.c
[guest@mslipatnikova ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Figure 7: Чтение readfile.c

```
[root@mslipatnikova ~]# chown root /home/guest/readfile.c
[root@mslipatnikova ~]# chmod 700 /home/guest/readfile.c
[root@mslipatnikova ~]# chown root:guest /home/guest/readfile
[root@mslipatnikova ~]# chmod u+s /home/guest/readfile
[root@mslipatnikova ~]# chmod g+s /home/guest/readfile
```

Figure 8: Команды от суперпользователя

Выполнение лабораторной работы

Figure 9: Чтение с помощью программы readfile

Выполнение лабораторной работы

```
[guest@mslipatnikova ~]$ ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 Oct  8 17:10 tmp
[guest@mslipatnikova ~]$ echo "test" > /tmp/file01.txt
[guest@mslipatnikova ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 17:18 /tmp/file01.txt
[guest@mslipatnikova ~]$ chmod o+rw /tmp/file01.txt
[guest@mslipatnikova ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 17:18 /tmp/file01.txt
[guest@mslipatnikova ~]$ su guest2
Password:
[guest2@mslipatnikova guest]$ echo "test2">>/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test
test2
[guest2@mslipatnikova guest]$ echo "test3">/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test3
[guest2@mslipatnikova guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Figure 10: Работа с tmp/file01.txt

Выполнение лабораторной работы

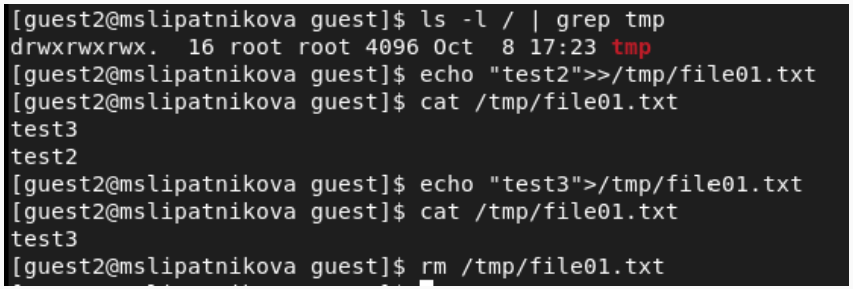


Figure 11: Работа с tmp/file01.txt без t

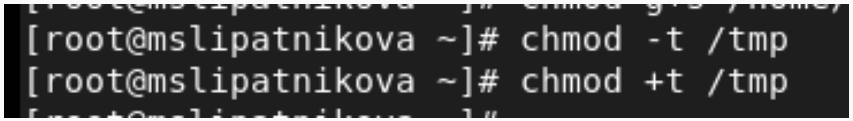


Figure 12: Команды от суперпользователя

Результат выполнения работы

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

Список литературы

1. Теоретические материалы курса.