

Лабораторная работа №5

Василий О. Худицкий

РУДН, 8 октября 2022, Москва, Россия

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.

Задание лабораторной работы

- Выполнить задания лабораторной работы.
- Проанализировать полученные результаты.

Выполнение лабораторной работы

simpleid

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

Рис.1 Выполнение simpleid.c и id

simpleid2

```
#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;
}
```

```
[guest@vokhudickiyj ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@vokhudickiyj ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис.2 Выполнение simpleid2 и id

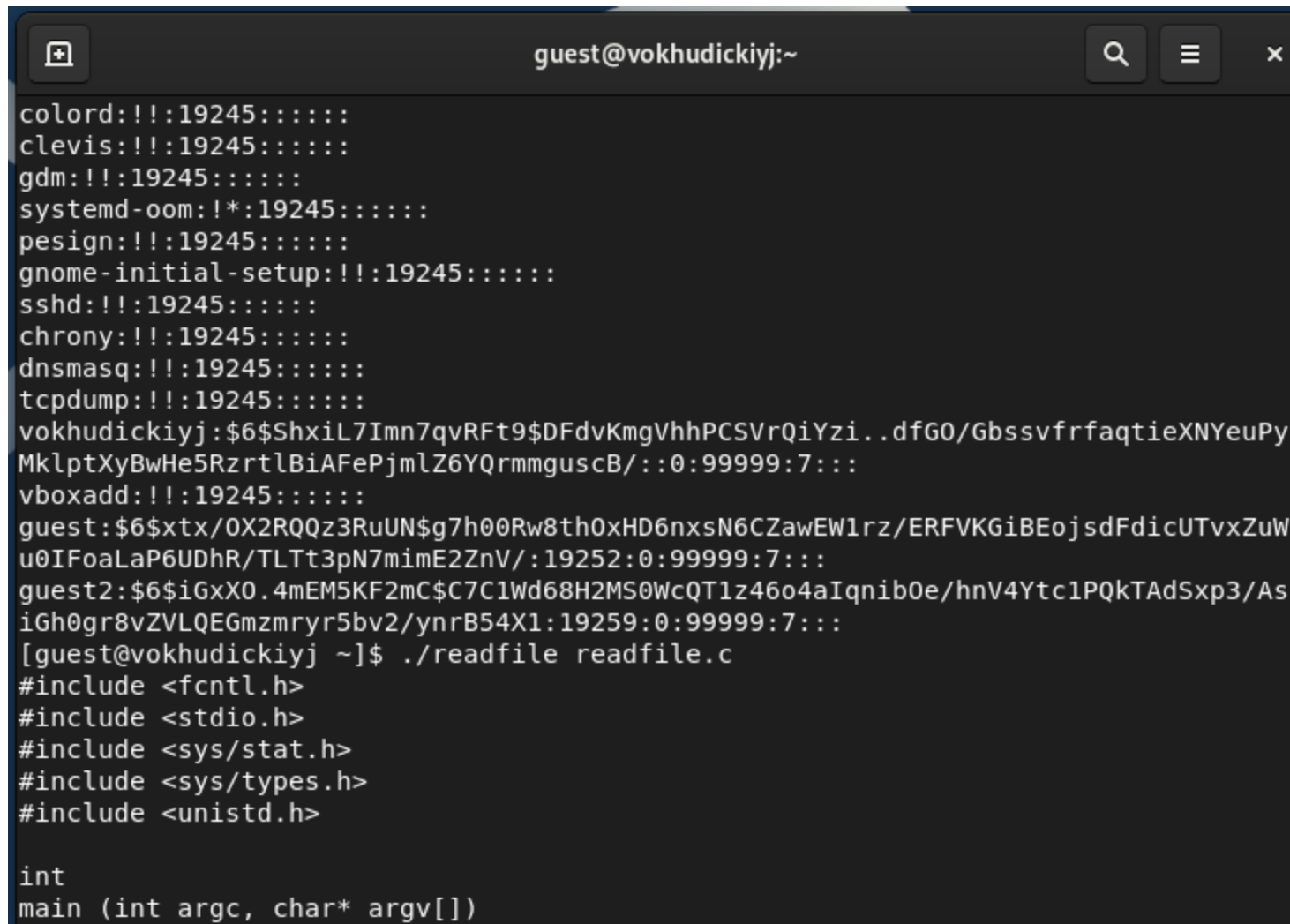
readfile

```
#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@vokhudickiyj:~
colord:!!:19245::::::
clevis:!!:19245::::::
gdm:!!:19245::::::
systemd-oom:!*:19245::::::
pesign:!!:19245::::::
gnome-initial-setup:!!:19245::::::
sshd:!!:19245::::::
chrony:!!:19245::::::
dnsmasq:!!:19245::::::
tcpdump:!!:19245::::::
vokhudickiyj:$6$ShxiL7Imn7qvRft9$DFdvKmgVhhPCSVrQiYzi..dfG0/GbssvfrfaqtieXNYeuPy
MklptXyBwHe5RzrtlBiAFepjmlZ6YQrmmguscB/::0:99999:7::
vboxadd:!!:19245::::::
guest:$6$xtx/OX2RQQz3RuUN$g7h00Rw8th0xHD6nxsN6CZawEW1rz/ERFVKGiBEojdFdicUTvxZuW
u0IFoaLaP6UDhR/TLTt3pN7mimE2ZnV/:19252:0:99999:7::
guest2:$6$iGxX0.4mEM5KF2mC$C7C1Wd68H2MS0wcQT1z46o4aIqnib0e/hnV4Ytc1PQkTAdSxp3/As
iGh0gr8vZVLQEGmzmryr5bv2/ynrB54X1:19259:0:99999:7::
[guest@vokhudickiyj ~]$ ./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[])
```

Рис.3 Чтение файлов /etc/shadow и readfile.c

Работа со Sticky-битом

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

Рис.4 Действия с файлом с атрибутом t от имени guest2

Работа после снятия Sticky-бита

```
[guest2@vokhudickiyj guest]$ su
Password:
[root@vokhudickiyj guest]# chmod -t /tmp
[root@vokhudickiyj guest]# exit
exit
[guest2@vokhudickiyj guest]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  8 17:10 tmp
[guest2@vokhudickiyj guest]$ cat /tmp/file01.txt
test3
[guest2@vokhudickiyj guest]$ echo "test2" > /tmp/file01.txt
[guest2@vokhudickiyj guest]$ cat /tmp/file01.txt
test2
[guest2@vokhudickiyj guest]$ echo "test3" > /tmp/file01.txt
[guest2@vokhudickiyj guest]$ cat /tmp/file01.txt
test3
[guest2@vokhudickiyj guest]$ rm /tmp/file01.txt
```

Рис.5 Действия с файлом без атрибута t от имени guest2

Возвращение атрибута t директории /tmp

```
[guest2@vokhudickiyj guest]$ su
Password:
[root@vokhudickiyj guest]# chmod +t /tmp
[root@vokhudickiyj guest]# exit
exit
[guest2@vokhudickiyj guest]$
```

Рис.6 Возвращение атрибута t

Выводы

В результате выполнения лабораторных работ я

- изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов;
- рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.