

Презентация по лабораторной работе №5

Калинин Тимур Дмитриевич

РУДН

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

Создание программы

```
1  #include <sys/types.h>
2  #include <unistd.h>
3  #include <stdio.h>
4
5  int main ()
6  {
7      uid_t real_uid = getuid();
8      uid_t e_uid = geteuid();
9
10     gid_t real_gid = getgid();
11     gid_t e_gid = getegid();
12
13
14     printf ("uid=%d, gid=%d\n", e_uid, e_gid);
15     printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
16     return 0;
17 }
```

Figure 1: Код simpleid2.c

```
[guest@tdkalinin lab5]$ gcc simpleid2.c -o simpleid2
[guest@tdkalinin lab5]$ ./simpleid2
uid=1001, gid=1001
real_uid=1001, real_gid=1001
[guest@tdkalinin lab5]$
```

Figure 2: Компиляция и выполнение simpleid2.c

```
[root@tdkalinin ~]# chown root:guest /home/guest/ib/lab5/simpleid2
[root@tdkalinin ~]# chown u+s /home/guest/ib/lab5/simpleid2
chown: неверный пользователь: «u+s»
[root@tdkalinin ~]# chmod u+s /home/guest/ib/lab5/simpleid2
[root@tdkalinin ~]#
```

Figure 3: Установка прав

```
[guest@tdkalinin lab5]$ ./simpleid2  
uid=0, gid=1001  
real_uid=1001, real_gid=1001  
[guest@tdkalinin lab5]$
```

Figure 4: Запуск simpleid2


```
[root@tdkalinin lab5]# chmod g+s /home/guest/ib/lab5/simpleid2
[root@tdkalinin lab5]# sudo guest2
sudo: guest2: command not found
[root@tdkalinin lab5]# su guest2
[guest2@tdkalinin lab5]$ cd ~/ib/lab5
bash: cd: /home/guest2/ib/lab5: Нет такого файла или каталога
[guest2@tdkalinin lab5]$ cd /home/guest/ib/lab5
[guest2@tdkalinin lab5]$ ./simpleid2
uid=0, gid=1001
real_uid=1002, real_gid=1002
```

Figure 5: Установка setGID-бита

```
1  #include <fcntl.h>
2  #include <stdio.h>
3  #include <sys/stat.h>
4  #include <sys/types.h>
5  #include <unistd.h>
6  int main (int argc, char* argv[])
7  {
8      unsigned char buffer[16];
9      size_t bytes_read;
10     int i;
11     int fd = open(argv[1], O_RDONLY);
12     do
13     {
14         bytes_read = read(fd, buffer, sizeof (buffer));
15         for (i =0; i < bytes_read; ++i) printf("%c", buffer[i]);
16     }
17     while (bytes_read == sizeof (buffer));
18     close (fd);
19     return 0;
20 }
```

Figure 6: Код readfile.c

```
[root@tdkalinin ~]# chown root:root /home/guest/ib/lab5/readfile.c  
[root@tdkalinin ~]# ls -l /home/guest/ib/lab5/readfile.c  
-rw-rw-r--. 1 root root 455 окт  3 14:47 /home/guest/ib/lab5/readfile.c  
[root@tdkalinin ~]# chmod 660 /home/guest/ib/lab5/readfile.c
```

Figure 7: Изменяем владельца

```
[guest@tdkalinin root]$ cat /home/guest/ib/lab5/readfile.c  
cat: /home/guest/ib/lab5/readfile.c: Отказано в доступе
```

Figure 8: Проверка чтения

```
[root@tdkalinin ~]# chown root /home/guest/ib/lab5/readfile
```

Figure 9: Смена владельца

```
[root@tdkalinin ~]# chmod u+s /home/guest/ib/lab5/readfile
[root@tdkalinin ~]# ls -l /home/guest/ib/lab5/readfile
-rwsrwxr-x. 1 root guest 25952 окт  3 14:47 /home/guest/ib/lab5/readfile
[root@tdkalinin ~]#
```

Figure 10: Установка setUID-бита

```
[guest@tdkalinin lab5]$ ./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]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

Figure 11: Проверка чтения readfile.c

```
[guest@tdkalinin lab5]$ ./readfile /etc/shadow
root:$6$tRKR2YvsF9HrcmrE$uQGkswcl7ITg6c7ZtsQj4IeSmtMs0TnIYX0ewZVJtlvmc7gs1
27ie77GsCbJzm51EBoI1syXTqaHpbBq1::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:::
ftp:*.19123:0:99999:7:::
nobody:*.19123:0:99999:7:::
systemd-coredump:!!:19241:::
dbus:!!:19241:::
polkitd:!!:19241:::
rtkit:!!:19241:::
sssd:!!:19241:::
avahi:!!:19241:::
pipewire:!!:19241:::
libstoragemgmt:!!:19241:::
```

Figure 12: Проверка чтения /etc/shadow


```
[guest@tdkalinin ~]$ ls -l / | grep tmp  
drwxrwxrwt. 24 root root 4096 окт 3 15:26 tmp
```

Figure 13: Атрибуты

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

Figure 14: Создание нового файла

```
[guest@tdkalinin ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 окт  3 15:39 /tmp/file01.txt  
[guest@tdkalinin ~]$
```

Figure 15: Просмотр атрибутов

```
[guest@tdkalinin ~]$ chmod o+rw /tmp/file01.txt
```

Figure 16: Установка прав доступа

```
[guest2@tdkalinin guest]$ cat /tmp/file01.txt  
test  
[guest2@tdkalinin guest]$
```

Figure 17: Чтение файла

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

Figure 18: Дозапись в файл

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

Figure 19: Перезапись файла

```
[guest2@tdkalinin guest]$ cat /tmp/file01.txt  
test3  
[guest2@tdkalinin guest]$
```

Figure 20: Проверка содержимого


```
[guest2@tdkalinin guest]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@tdkalinin guest]$ su -
```

Figure 21: Попытка удаления

```
[root@tdkalinin ~]# chmod -t /tmp  
[root@tdkalinin ~]#
```

Figure 22: Снятие атрибута t

```
[guest2@tdkalinin root]$ echo "test2" >> /tmp/file01.txt
[guest2@tdkalinin root]$ cat /tmp/file01.txt
test3
test2
[guest2@tdkalinin root]$ echo "test2" > /tmp/file01.txt
[guest2@tdkalinin root]$ cat /tmp/file01.txt
test2
[guest2@tdkalinin root]$ rm /tmp/file01.txt
[guest2@tdkalinin root]$ █
```

Figure 23: Повтор действий

Итог

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