Презентация по лабораторной работе №5.

Основы информационной безопасности.

Рогожина Н.А.

13 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Рогожина Надежда Александровна
- Студентка 2го курса, НКАбд-02-22
- Компьютерные и информационные науки
- Российский университет дружбы народов
- Github

Вводная часть

Вводная часть

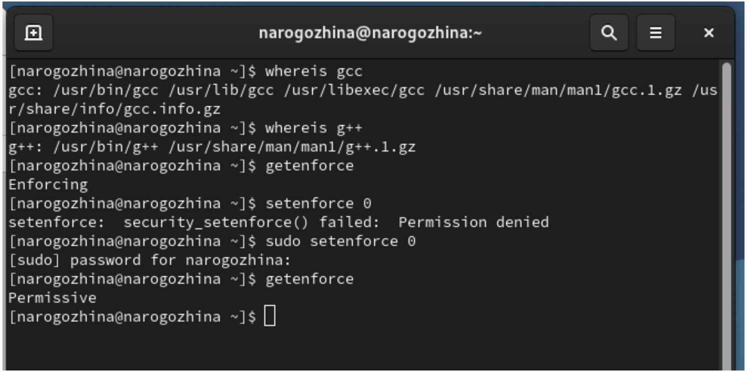
Объект и предмет исследования

- Права доступа к каталогам и файлам

Цели и задачи

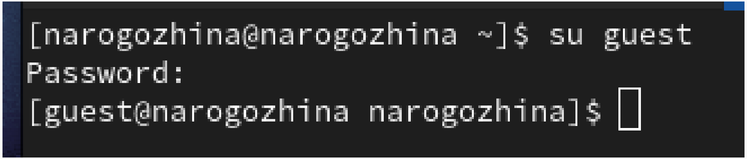
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Выполнение лабораторной работы



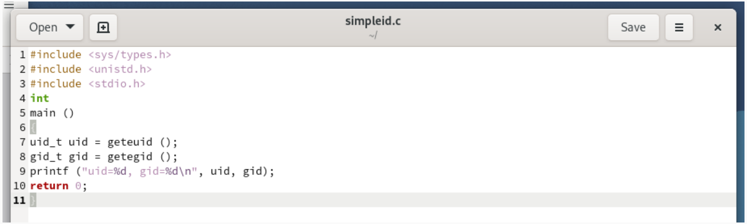
```
[narogozhina@narogozhina ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /us
r/share/info/gcc.info.gz
[narogozhina@narogozhina ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[narogozhina@narogozhina ~]$ getenforce
Enforcing
[narogozhina@narogozhina ~]$ setenforce 0
setenforce:  security_setenforce() failed:  Permission denied
[narogozhina@narogozhina ~]$ sudo setenforce 0
[sudo] password for narogozhina:
[narogozhina@narogozhina ~]$ getenforce
Permissive
[narogozhina@narogozhina ~]$ 
```

Рис. 1: Вход в систему



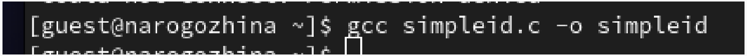
```
[narogozhina@narogozhina ~]$ su guest
Password:
[guest@narogozhina narogozhina]$ 
```

Рис. 2: Вход в систему



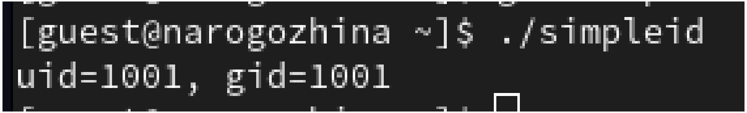
```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t uid = geteuid ();
gid_t gid = getegid ();
printf ("uid=%d, gid=%d\n", uid, gid);
return 0;
}
```

Рис. 3: simpleid.c



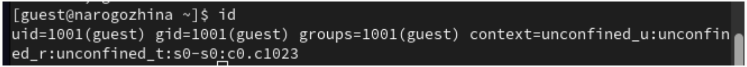
```
[guest@narogozhina ~]$ gcc simpleid.c -o simpleid
[guest@narogozhina ~]$ 
```

Рис. 4: компиляция



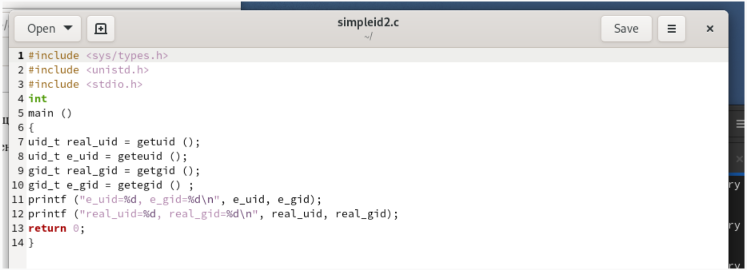
```
[guest@narogozhina ~]$ ./simpleid
uid=1001, gid=1001
```

Рис. 5: проверка работоспособности



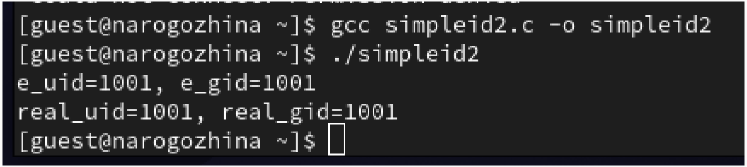
```
[guest@narogozhina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 6: id



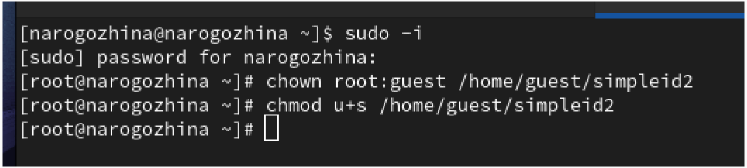
```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t real_uid = getuid ();
uid_t e_uid = geteuid ();
gid_t real_gid = getgid ();
gid_t e_gid = getegid () ;
printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
return 0;
}
```

Рис. 7: simpleid2.c



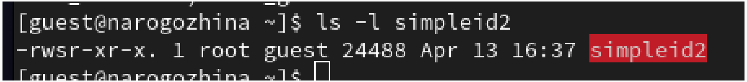
```
[guest@narogozhina ~]$ gcc simpleid2.c -o simpleid2
[guest@narogozhina ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@narogozhina ~]$ 
```

Рис. 8: simpleid2



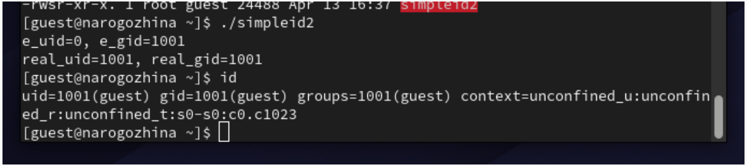
```
[narogozhina@narogozhina ~]$ sudo -i
[sudo] password for narogozhina:
[root@narogozhina ~]# chown root:guest /home/guest/simpleid2
[root@narogozhina ~]# chmod u+s /home/guest/simpleid2
[root@narogozhina ~]# 
```

Рис. 9: смена прав от root



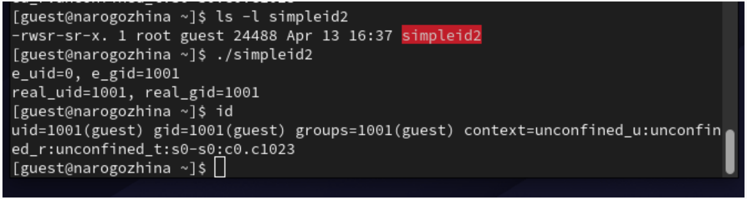
```
[guest@narogozhina ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 24488 Apr 13 16:37 simpleid2
[guest@narogozhina ~]$ 
```

Рис. 10: проверка



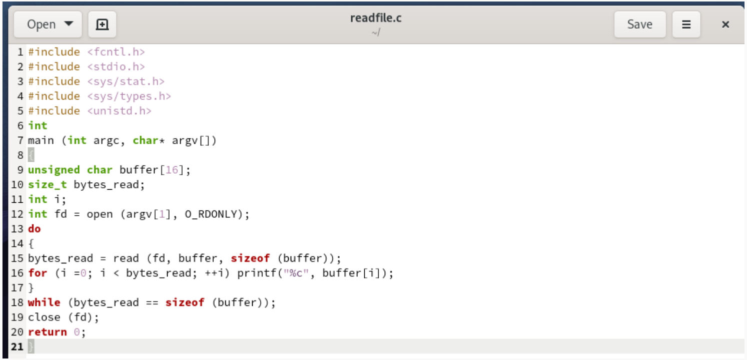
```
-rwsr-xr-x. 1 root guest 24488 Apr 13 16:37 simpleid2
[guest@narogozhina ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@narogozhina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@narogozhina ~]$ 
```

Рис. 11: id VS simpleid2



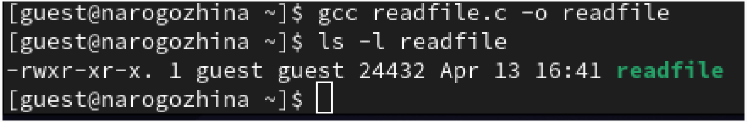
```
[guest@narogozhina ~]$ ls -l simpleid2
-rwsr-sr-x. 1 root guest 24488 Apr 13 16:37 simpleid2
[guest@narogozhina ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@narogozhina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@narogozhina ~]$ 
```

Рис. 12: SetGID-бит



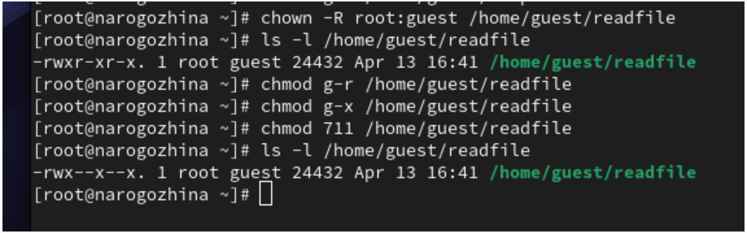
```c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
main (int argc, char* argv[])
{
unsigned char buffer[16];
size_t bytes_read;
int i;
int fd = open (argv[1], O_RDONLY);
do
{
bytes_read = read (fd, buffer, sizeof (buffer));
for (i =0; i < bytes_read; ++i) printf("%c", buffer[i]);
}
while (bytes_read == sizeof (buffer));
close (fd);
return 0;
}
```

Рис. 13: readfile



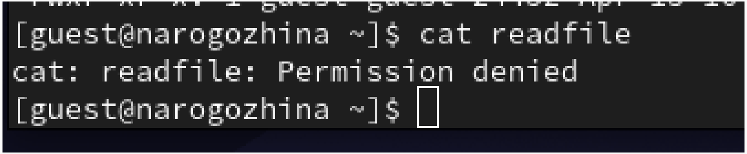
```
[guest@narogozhina ~]$ gcc readfile.c -o readfile
[guest@narogozhina ~]$ ls -l readfile
-rwxr-xr-x. 1 guest guest 24432 Apr 13 16:41 readfile
[guest@narogozhina ~]$ 
```

Рис. 14: компиляция и проверка прав



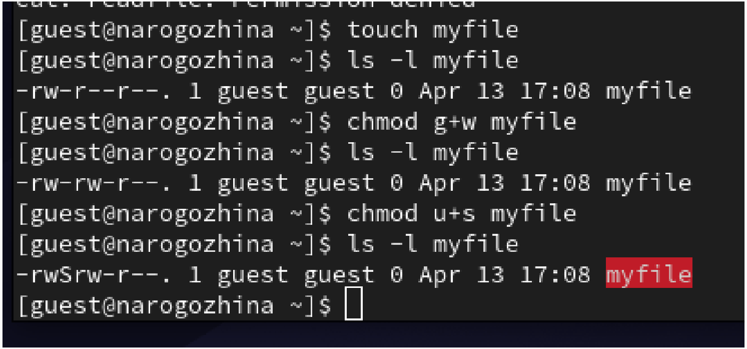
```
[root@narogozhina ~]# chown -R root:guest /home/guest/readfile
[root@narogozhina ~]# ls -l /home/guest/readfile
-rwxr-xr-x. 1 root guest 24432 Apr 13 16:41 /home/guest/readfile
[root@narogozhina ~]# chmod g-r /home/guest/readfile
[root@narogozhina ~]# chmod g-x /home/guest/readfile
[root@narogozhina ~]# chmod 711 /home/guest/readfile
[root@narogozhina ~]# ls -l /home/guest/readfile
-rwx--x--x. 1 root guest 24432 Apr 13 16:41 /home/guest/readfile
[root@narogozhina ~]# 
```

Рис. 15: Смена владельца и прав



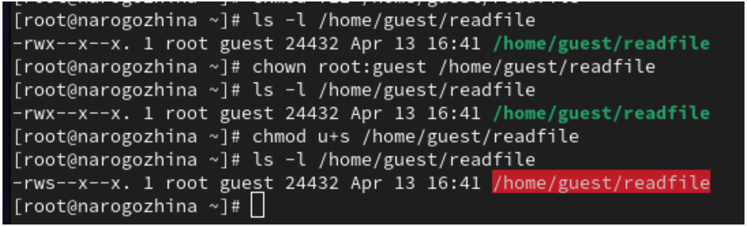
```
[guest@narogozhina ~]$ cat readfile
cat: readfile: Permission denied
[guest@narogozhina ~]$ 
```

Рис. 16: попытка №1



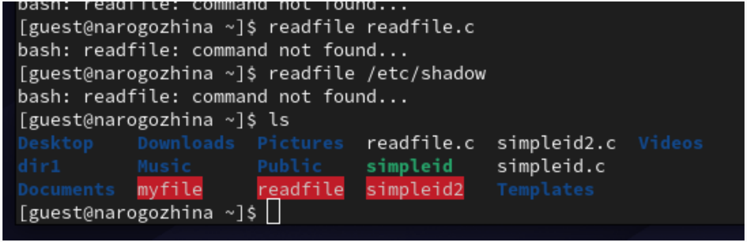
```
cat: readfile: Permission denied
[guest@narogozhina ~]$ touch myfile
[guest@narogozhina ~]$ ls -l myfile
-rw-r--r--. 1 guest guest 0 Apr 13 17:08 myfile
[guest@narogozhina ~]$ chmod g+w myfile
[guest@narogozhina ~]$ ls -l myfile
-rw-rw-r--. 1 guest guest 0 Apr 13 17:08 myfile
[guest@narogozhina ~]$ chmod u+s myfile
[guest@narogozhina ~]$ ls -l myfile
-rwSrw-r--. 1 guest guest 0 Apr 13 17:08 myfile
[guest@narogozhina ~]$ 
```

Рис. 17: SetUID



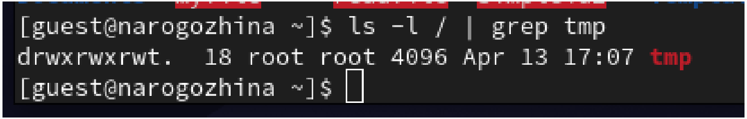
```
[root@narogozhina ~]# ls -l /home/guest/readfile
-rwx--x--x. 1 root guest 24432 Apr 13 16:41 /home/guest/readfile
[root@narogozhina ~]# chown root:guest /home/guest/readfile
[root@narogozhina ~]# ls -l /home/guest/readfile
-rwx--x--x. 1 root guest 24432 Apr 13 16:41 /home/guest/readfile
[root@narogozhina ~]# chmod u+s /home/guest/readfile
[root@narogozhina ~]# ls -l /home/guest/readfile
-rws--x--x. 1 root guest 24432 Apr 13 16:41 /home/guest/readfile
[root@narogozhina ~]# 
```

Рис. 18: смена владельца и прав



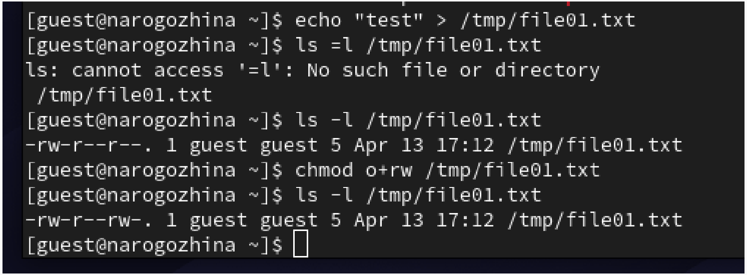
```
bash: readfile: command not found...
[guest@narogozhina ~]$ readfile readfile.c
bash: readfile: command not found...
[guest@narogozhina ~]$ readfile /etc/shadow
bash: readfile: command not found...
[guest@narogozhina ~]$ ls
Desktop    Downloads  Pictures  readfile.c  simpleid2.c  Videos
dir1       Music      Public    simpleid    simpleid.c
Documents  myfile     readfile  simpleid2   Templates
[guest@narogozhina ~]$ 
```

Рис. 19: попытка №2



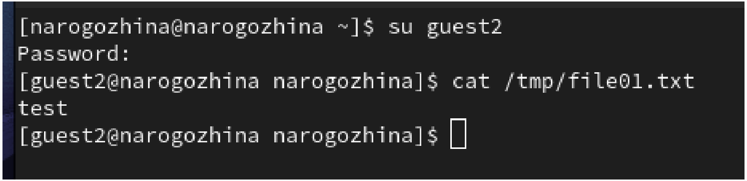
```
[guest@narogozhina ~]$ ls -l / | grep tmp
drwxrwxrwt.  18 root root 4096 Apr 13 17:07 tmp
[guest@narogozhina ~]$ 
```

Рис. 20: /tmp



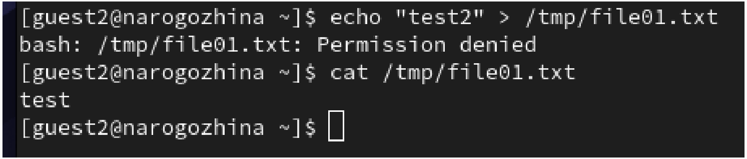
```
[guest@narogozhina ~]$ echo "test" > /tmp/file01.txt
[guest@narogozhina ~]$ ls =l /tmp/file01.txt
ls: cannot access '=l': No such file or directory
 /tmp/file01.txt
[guest@narogozhina ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Apr 13 17:12 /tmp/file01.txt
[guest@narogozhina ~]$ chmod o+rw /tmp/file01.txt
[guest@narogozhina ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Apr 13 17:12 /tmp/file01.txt
[guest@narogozhina ~]$ 
```

Рис. 21: file01.txt



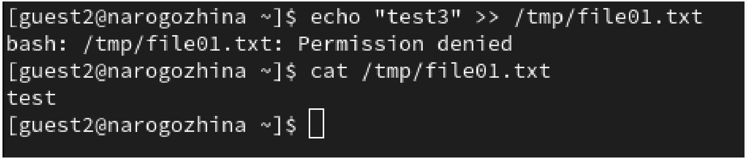
```
[narogozhina@narogozhina ~]$ su guest2
Password:
[guest2@narogozhina narogozhina]$ cat /tmp/file01.txt
test
[guest2@narogozhina narogozhina]$
```

Рис. 22: guest2



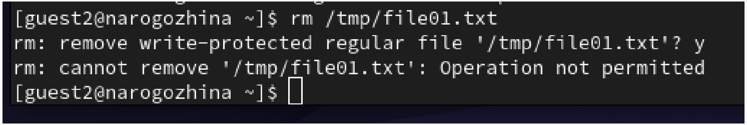
```
[guest2@narogozhina ~]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@narogozhina ~]$ cat /tmp/file01.txt
test
[guest2@narogozhina ~]$ 
```

Рис. 23: попытка №3



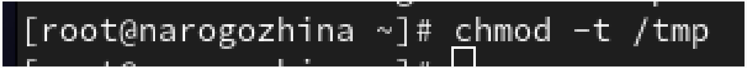
```
[guest2@narogozhina ~]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@narogozhina ~]$ cat /tmp/file01.txt
test
[guest2@narogozhina ~]$ 
```

Рис. 24: попытка №4



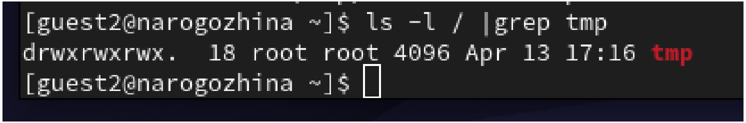
```
[guest2@narogozhina ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@narogozhina ~]$ 
```

Рис. 25: попытка №5

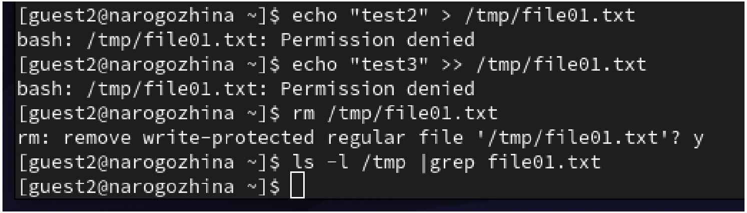


```
[root@narogozhina ~]# chmod -t /tmp
```

Рис. 26: смена прав /tmp

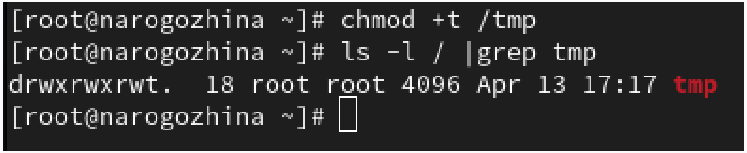


```
[guest2@narogozhina ~]$ ls -l / |grep tmp
drwxrwxrwx.  18 root root 4096 Apr 13 17:16 tmp
[guest2@narogozhina ~]$ 
```



```
[guest2@narogozhina ~]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@narogozhina ~]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@narogozhina ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@narogozhina ~]$ ls -l /tmp |grep file01.txt
[guest2@narogozhina ~]$ 
```

Рис. 27: повтор



```
[root@narogozhina ~]# chmod +t /tmp
[root@narogozhina ~]# ls -l / |grep tmp
drwxrwxrwt.  18 root root 4096 Apr 13 17:17 tmp
[root@narogozhina ~]# 
```

Рис. 28: возвращение прав