

Отчет к лабораторной работе №5

Common information

discipline: Основы информационной безопасности group: НПМбд-02-21

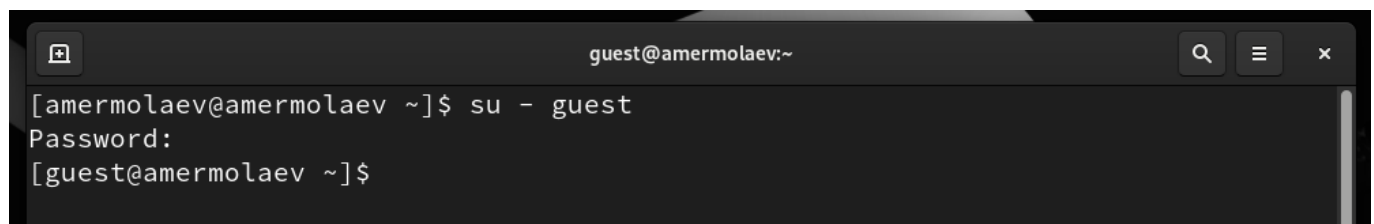
author: Ермолаев А.М.

Цель работы

- Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
- Получить практический навык работы в консоли с дополнительными атрибутами.
- Рассмотреть работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Выполнение работы

Войдем в систему от имени пользователя guest^



```
guest@amermolaev:~  
[amermolaev@amermolaev ~]$ su - guest  
Password:  
[guest@amermolaev ~]$
```

Создадим программу simpleid.c:



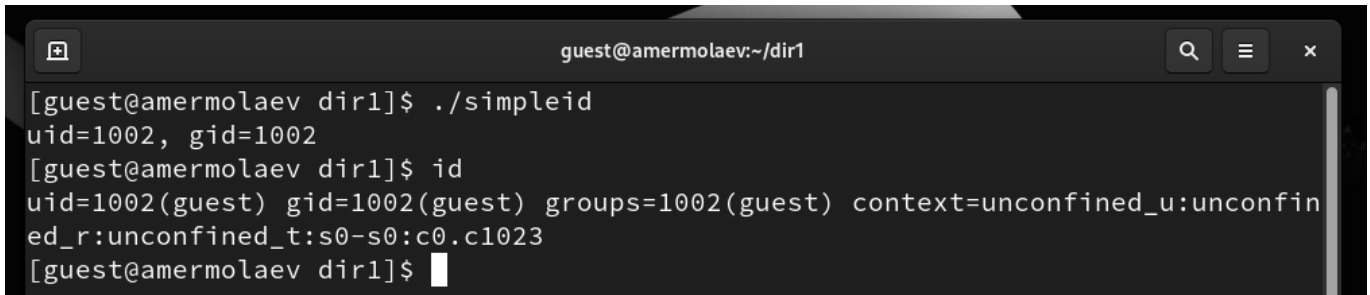
```
GNU nano 5.6.1 simpleid.c  
#include <sys/types.h>  
#include <unistd.h>  
#include <stdio.h>  
int main ()  
{  
    uid_t uid = geteuid ();  
    gid_t gid = getegid ();  
    printf ("uid=%d, gid=%d\n", uid, gid);  
    return 0;  
}
```

Скомпилируем программу и убедимся, что файл программы создан:



```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ gcc simpleid.c -o simpleid
[guest@amermolaev dir1]$ ls
file1  simpleid  simpleid.c
[guest@amermolaev dir1]$
```

Выполним программу simpleid и системную программу id:



```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ ./simpleid
uid=1002, gid=1002
[guest@amermolaev dir1]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@amermolaev dir1]$
```

Усложним программу, добавив вывод действительных идентификаторов. Получившуюся программу назовем simpleid2.c:



```
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;
}
```

Скомпилируем и запустим simpleid2.c:



```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ gcc simpleid2.c -o simpleid2
[guest@amermolaev dir1]$ ls
file1  simpleid  simpleid2  simpleid2.c  simpleid.c
[guest@amermolaev dir1]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest@amermolaev dir1]$
```

От имени суперпользователя выполним команды:

```
amermolaev@amermolaev:~$ sudo chown root:guest /home/guest/dir1/simpleid2
[amermolaev@amermolaev ~]$ sudo chmod u+s /home/guest/dir1/simpleid2
[amermolaev@amermolaev ~]$ ls -l /home/guest/dir1/simpleid2
ls: cannot access '/home/guest/dir1/simpleid2': Permission denied
[amermolaev@amermolaev ~]$ sudo ls -l /home/guest/dir1/simpleid2
-rwsr-xr-x. 1 root guest 24488 Sep 30 21:52 /home/guest/dir1/simpleid2
[amermolaev@amermolaev ~]$
```

Запустим simpleid2 и id:

```
guest@amermolaev:~/dir1$ ./simpleid2
e_uid=0, e_gid=1002
real_uid=1002, real_gid=1002
[guest@amermolaev dir1]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@amermolaev dir1]$
```

Прделаем тоже самое относительно SetGID-бита:

```
guest@amermolaev:~/dir1$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest@amermolaev dir1]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@amermolaev dir1]$
```

```
amermolaev@amermolaev:~$ sudo chown root:guest /home/guest/dir1/simpleid2
[sudo] password for amermolaev:
[amermolaev@amermolaev ~]$ sudo chmod g+s /home/guest/dir1/simpleid2
[amermolaev@amermolaev ~]$
```

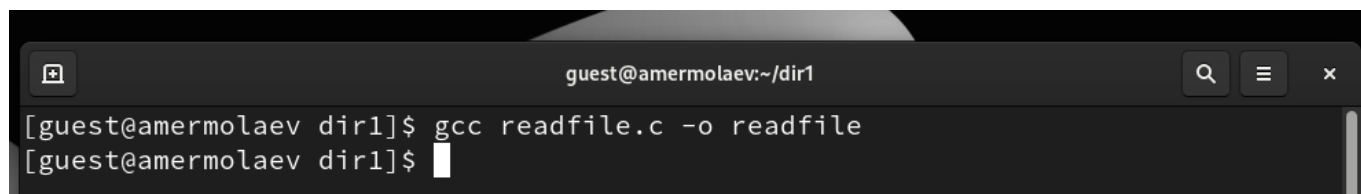
Создадим программу readfile.c:



```
GNU nano 5.6.1 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;
}

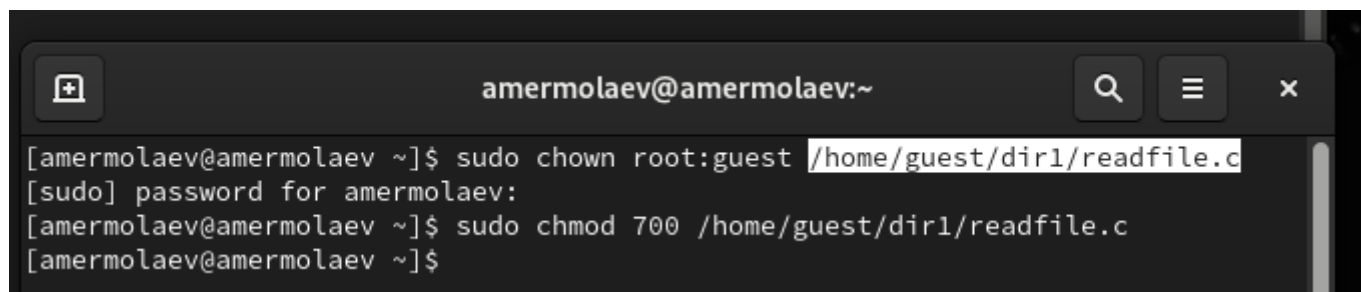
[ Read 20 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Скомпилируем её:



```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ gcc readfile.c -o readfile
[guest@amermolaev dir1]$
```

Сменим владельца у файла readfile.c (или любого другого текстового файла в системе) и изменим права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог:



```
amermolaev@amermolaev:~
[amermolaev@amermolaev ~]$ sudo chown root:guest /home/guest/dir1/readfile.c
[sudo] password for amermolaev:
[amermolaev@amermolaev ~]$ sudo chmod 700 /home/guest/dir1/readfile.c
[amermolaev@amermolaev ~]$
```

Проверим, что пользователь guest не может прочитать файл readfile.c. Сменим у программы readfile владельца и установим SetU'D-бит:

```

guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@amermolaev dir1]$

amermolaev@amermolaev:~
[amermolaev@amermolaev ~]$ sudo chown root:guest /home/guest/dir1/readfile.c
[sudo] password for amermolaev:
[amermolaev@amermolaev ~]$ sudo chmod 700 /home/guest/dir1/readfile.c
[amermolaev@amermolaev ~]$

```

Проверим, может ли программа readfile прочитать файл readfile.c:

```

guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ ./readfile readfile.c
[amermolaev@amermolaev ~]$ sudo chown root:guest /home/guest/dir1/readfile.c
[sudo] password for amermolaev:
[amermolaev@amermolaev ~]$ sudo chmod u+s /home/guest/dir1/readfile.c
[amermolaev@amermolaev ~]$

amermolaev@amermolaev:~
STCONTROL=guestXAU
ORS=rs=0:
3;01:or=4

```

Проверим, может ли программа readfile прочитать файл /etc/shadow:

```

guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ ./readfile /etc/shadow
#]tV@hk[...C`[...t...@
...tp@`k...xk...
pI]t...pe...!...@e8

C3q0...>x86_64./readfile/etc/shadowSHELL=/bin/bashHISTCON
TROL=ignoredupsHISTSIZE=1000HOSTNAME=amermolaevPWD=/home/guest/dir1LOGNAME=gues
tXAUTHORITY=/home/guest/.xauthlqytjXHOME=/home/guestLANG=en_GB.UTF-8LS_COLORS=r
s=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:
or=40;31;01:mi=01;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:e
x=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31
:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z
=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lzo=01;31:*.xz
=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.
.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01

```

Выясним, установлен ли атрибут Sticky на директории /tmp:

```

guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Sep 30 22:32 tmp
[guest@amermolaev dir1]$

```

От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test:

```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ echo "test" > /tmp/file01.txt
[guest@amermolaev dir1]$ ls /tmp
file01.txt
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-chrond.service-8Fu5nX
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-colord.service-IXfxDZ
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-dbus-broker.service-21Mvmg
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-fwupd.service-cArJJj
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-ModemManager.service-BhDSqF
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-power-profiles-daemon.service-mAL6Ke
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-rtkit-daemon.service-3qtdyQ
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-switcheroo-control.service-fTigAx
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-systemd-logind.service-1vEfq4
systemd-private-5ec4b3a35a6d4ec29306967e1a7816c2-upower.service-kjWEHt
[guest@amermolaev dir1]$
```

Посмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные»:

```
guest@amermolaev:~/dir1
[guest@amermolaev dir1]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Sep 30 22:33 /tmp/file01.txt
[guest@amermolaev dir1]$ chmod o+rw /tmp/file01.txt
[guest@amermolaev dir1]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Sep 30 22:33 /tmp/file01.txt
[guest@amermolaev dir1]$
```

От пользователя guest2 (не являющегося владельцем) попробуем прочитать файл /tmp/file01.txt, а также дозаписать в файл слово test2:

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

Также попробуем записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию:

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

От пользователя guest2 попробуем удалить файл /tmp/file01.txt:

```
guest2@amermolaev:~  
[guest2@amermolaev ~]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': No such file or directory  
[guest2@amermolaev ~]$
```

Повысим свои права до суперпользователя и выполним после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp:

```
amermolaev@amermolaev:~  
[amermolaev@amermolaev ~]$ su -  
Password:  
[root@amermolaev ~]# chmod -t /tmp  
[root@amermolaev ~]# exit  
logout
```

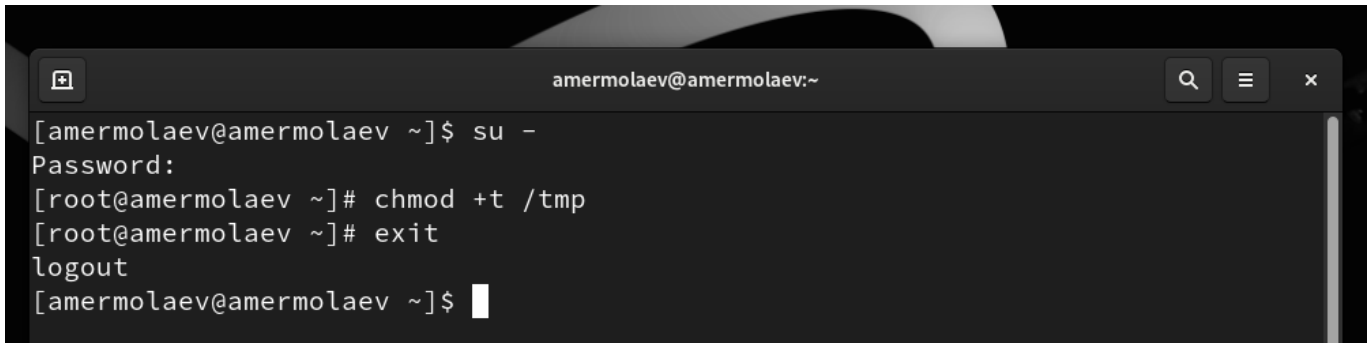
От пользователя guest2 проверим, что атрибута t у директории /tmp нет:

```
guest2@amermolaev:~  
[guest2@amermolaev ~]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 Sep 30 22:43 tmp  
[guest2@amermolaev ~]$
```

Повторим предыдущие шаги:

```
guest2@amermolaev:~  
[guest2@amermolaev ~]$ cat /tmp/file01.txt  
test  
[guest2@amermolaev ~]$ echo "test2" > /tmp/file01.txt  
-bash: /tmp/file01.txt: Permission denied  
[guest2@amermolaev ~]$ cat /tmp/file01.txt  
test  
[guest2@amermolaev ~]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': No such file or directory  
[guest2@amermolaev ~]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': No such file or directory  
[guest2@amermolaev ~]$ echo "test3" > /tmp/file01.txt
```

Повысим свои права до суперпользователя и верните атрибут t на директорию /tmp:



```
amermolaev@amermolaev:~  
[amermolaev@amermolaev ~]$ su -  
Password:  
[root@amermolaev ~]# chmod +t /tmp  
[root@amermolaev ~]# exit  
logout  
[amermolaev@amermolaev ~]$
```

Вывод

В рамках выполнения работы я

- Изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
- Получил практический навык работы в консоли с дополнительными атрибутами.
- Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

- <https://rockylinux.org/>
- <https://habr.com/ru/articles/469667/>
- <https://www.golinuxcloud.com/sticky-bit-linux/>