

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.

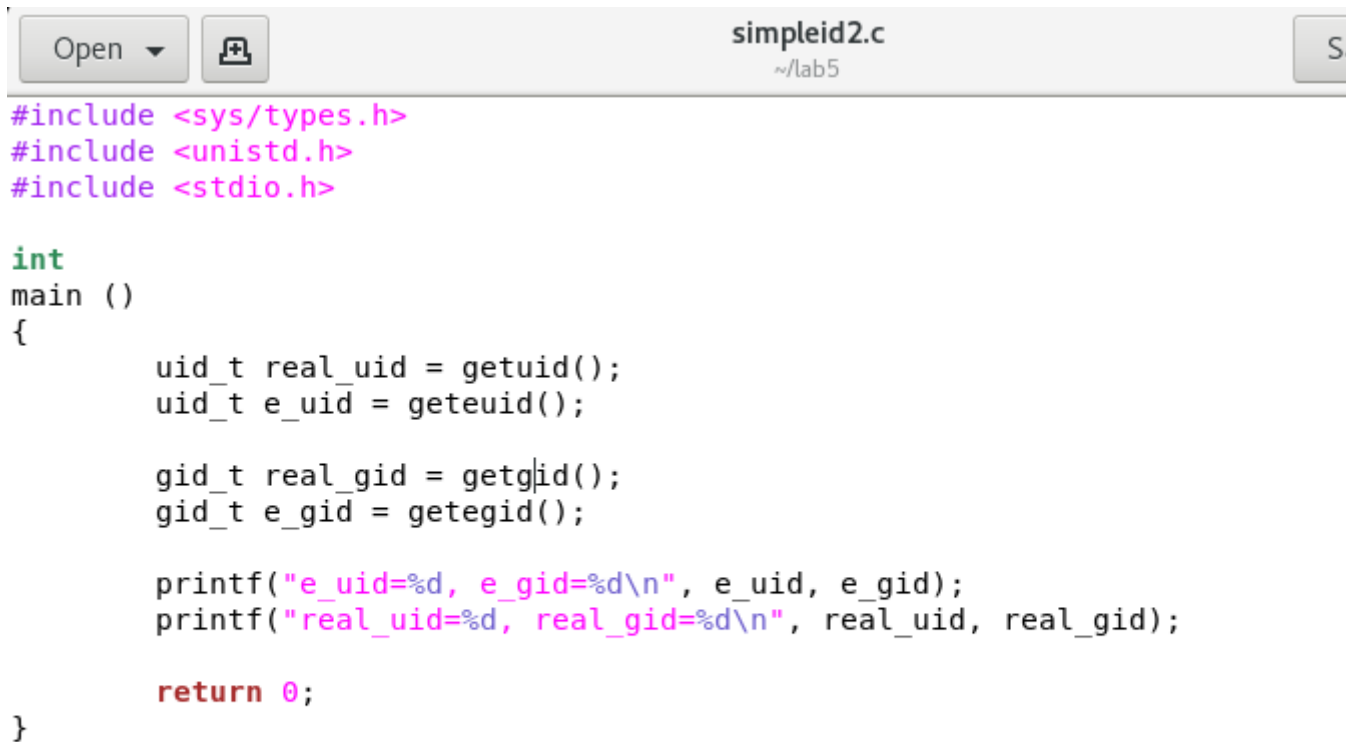
Выполнение лабораторной работы

Входим в систему от guest и создаем программу simpleid.c

Листинг программы simpleid [fig:2].

{#fig:2 width=100%}

Усложните программу, добавив вывод действительных идентификаторов и назовите ее simpleid2 [fig:4]



```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t real_uid = getuid();
    uid_t e_uid = geteuid();

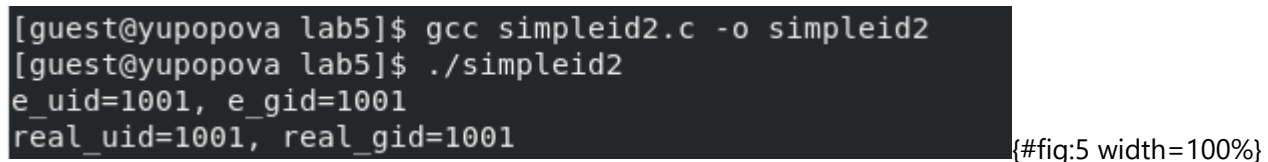
    gid_t real_gid = getgid();
    gid_t e_gid = getegid();

    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;
}
```

{#fig:4 width=100%}

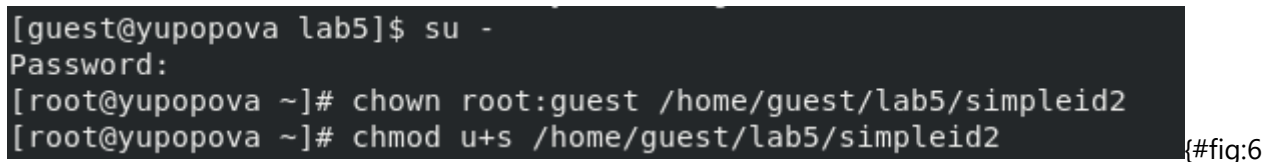
Скомпилируйте и запустите simpleid2.c [﻿@fig:5]



```
[guest@yupopova lab5]$ gcc simpleid2.c -o simpleid2
[guest@yupopova lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

{#fig:5 width=100%}

От имени суперпользователя выполните команды: `chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2` [﻿@fig:6].



```
[guest@yupopova lab5]$ su -
Password:
[root@yupopova ~]# chown root:guest /home/guest/lab5/simpleid2
[root@yupopova ~]# chmod u+s /home/guest/lab5/simpleid2
```

{#fig:6

width=100%}

Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2: `ls -l simpleid2` Запустите simpleid2 и id: `./simpleid2 id` [﻿@fig:7].

```
[guest@yupopova lab5]$ lsattr
----- ./simpleid.c
----- ./simpleid2.c
----- ./readfile.c
----- ./simpleid
----- ./simpleid2
[guest@yupopova lab5]$ ls -l
total 52
-rw-rw-r--. 1 guest guest  411 Oct  8 08:10 readfile.c
-rwxrwxr-x. 1 guest guest 18096 Oct  8 08:54 simpleid
-rwsrwxr-x. 1 root  guest 18256 Oct  8 09:00 simpleid2
-rw-rw-r--. 1 guest guest  307 Oct  8 08:59 simpleid2.c
-rw-rw-r--. 1 guest guest  178 Oct  8 08:54 simpleid.c
[guest@yupopova lab5]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 18256 Oct  8 09:00 simpleid2
```

{#fig:7}

width=100%}

Проделайте тоже самое относительно SetGID-бита [﻿@fig:1] [﻿@fig:8]

```
[root@yupopova ~]# chmod g+s /home/guest/lab5/simpleid2
```

{#fig:1 width=100%}

```
[guest@yupopova lab5]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 18256 Oct  8 09:00 simpleid2
[guest@yupopova lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@yupopova lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yupopova lab5]$ ls -l
total 52
-rw-rw-r--. 1 guest guest  411 Oct  8 08:10 readfile.c
-rwxrwxr-x. 1 guest guest 18096 Oct  8 08:54 simpleid
-rwsrwxr-x. 1 root  guest 18256 Oct  8 09:00 simpleid2
-rw-rw-r--. 1 guest guest  307 Oct  8 08:59 simpleid2.c
-rw-rw-r--. 1 guest guest  178 Oct  8 08:54 simpleid.c
[guest@yupopova lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

{#fig:8 width=100%}

Создайте программу readfile.c [﻿@fig:9].

```
[guest@yupopova lab5]$ 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;
}
```

{#fig:9 width=100%}

Смените владельца у файла readfile.c и измените права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог [fig:10].

```
[root@yupopova ~]# chown root:guest /home/guest/lab5/readfile
[root@yupopova ~]# chmod 700 /home/guest/lab5/readfile
chmod: cannot access '/home/guest/lab5/readfile': No such file or directory
[root@yupopova ~]# chmod 700 /home/guest/lab5/readfile.c
chmod: cannot access '/home/guest/lab5/readfile.c': No such file or directory
[root@yupopova ~]# chmod 700 /home/guest/lab5/readfile.c
```

{#fig:10 width=100%}

Проверьте, что пользователь guest не может прочитать файл readfile.c. Смените у программы readfile владельца и установите SetU'D-бит. [fig:11].

```
[root@yupopova ~]# chown guest:guest /home/guest/lab5/readfile
```

{#fig:11

width=100%}

Проверьте, может ли программа readfile прочитать файл readfile.c? [fig:12]

```
[guest@yupopova 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));
}
```

{#fig:12 width=100%}

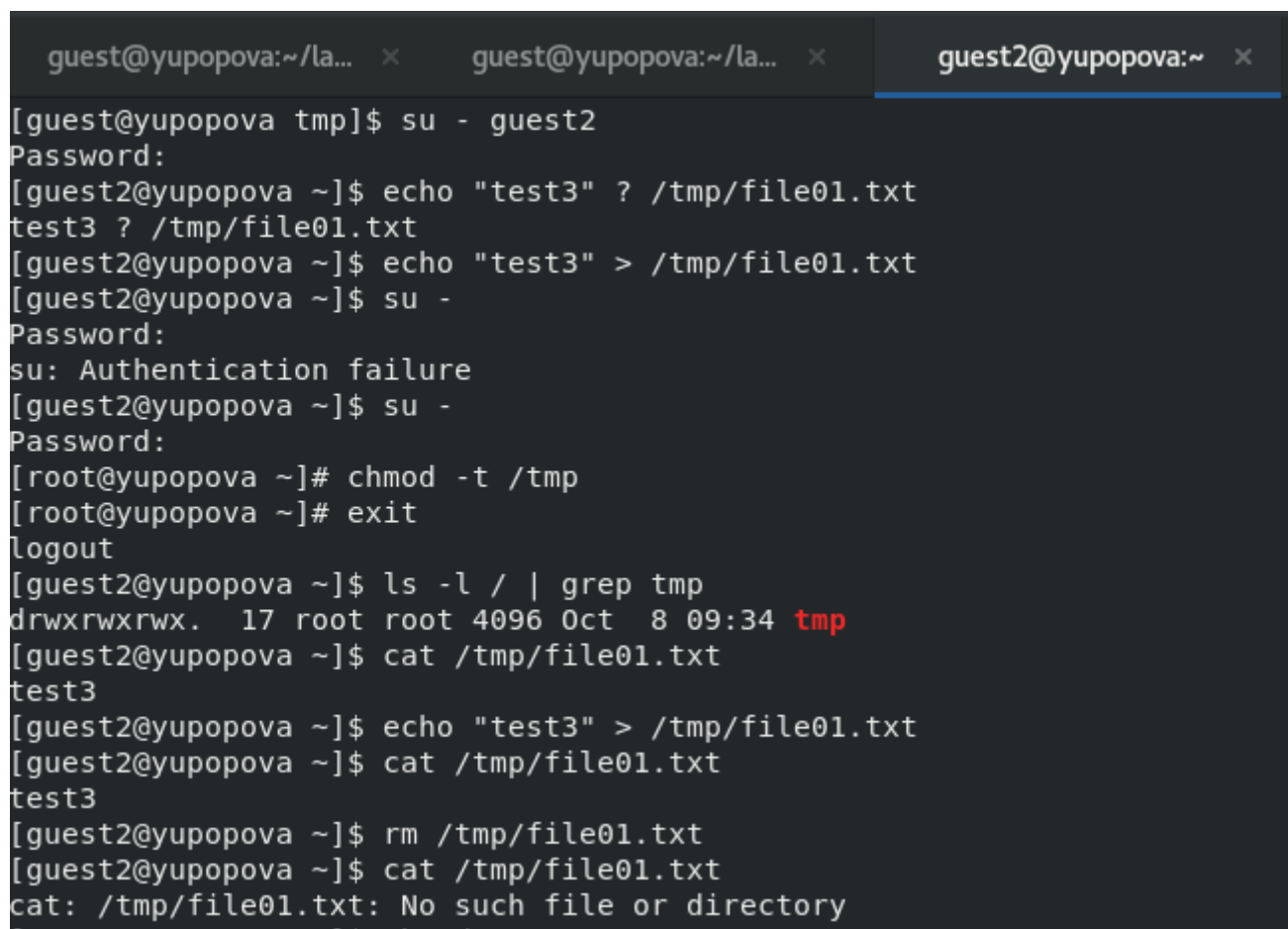
Выясните, установлен ли атрибут Sticky на директории /tmp От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test: Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» [afig:13]

```
[guest@yupopova lab5]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct  8 09:19 tmp
[guest@yupopova lab5]$ cd ..
[guest@yupopova ~]$ pwd
/home/guest
[guest@yupopova ~]$ cd ..
[guest@yupopova home]$ cd ..
[guest@yupopova /]$ pwd
/
[guest@yupopova /]$ cd tmp
[guest@yupopova tmp]$ pwd
/tmp
[guest@yupopova tmp]$ touch file01.txt
[guest@yupopova tmp]$ ls
file01.txt
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-chrond.service-2nNG3h
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-colord.service-aG5wzh
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-fwupd.service-oPtZzf
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-geoclue.service-9iwhmf
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-ModemManager.service-gPZL9h
systemd-private-1d0a58bd843c4b0790c18fdde62d8b25-rtkit-daemon.service-E9htYh
tracker-extract-files.1000
tracker-extract-files.1001
[quest@yupopova tmp]$ echo "test" > /tmp/file.txt
```

{#fig:13 width=100%}

От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 Проверьте содержимое

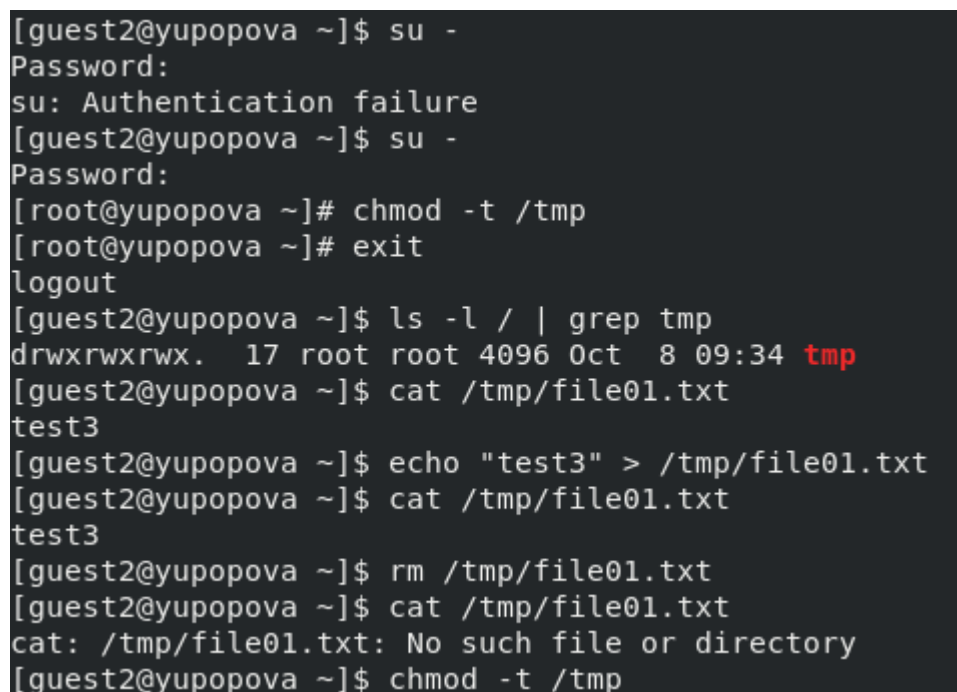
файла От пользователя guest2 попробуйте записать в файл /tmp/file01.txt Проверьте содержимое файла
От пользователя guest2 попробуйте удалить файл /tmp/file01.txt [@fig:14]



```
guest@yupopova:~/la... x  guest@yupopova:~/la... x  guest2@yupopova:~ x
[guest@yupopova tmp]$ su - guest2
Password:
[guest2@yupopova ~]$ echo "test3" ? /tmp/file01.txt
test3 ? /tmp/file01.txt
[guest2@yupopova ~]$ echo "test3" > /tmp/file01.txt
[guest2@yupopova ~]$ su -
Password:
su: Authentication failure
[guest2@yupopova ~]$ su -
Password:
[root@yupopova ~]# chmod -t /tmp
[root@yupopova ~]# exit
logout
[guest2@yupopova ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 Oct  8 09:34 tmp
[guest2@yupopova ~]$ cat /tmp/file01.txt
test3
[guest2@yupopova ~]$ echo "test3" > /tmp/file01.txt
[guest2@yupopova ~]$ cat /tmp/file01.txt
test3
[guest2@yupopova ~]$ rm /tmp/file01.txt
[guest2@yupopova ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
```

{#fig:14 width=100%}

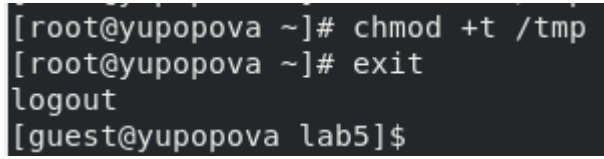
Повысьте свои права до суперпользователя и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp От пользователя guest2 проверьте, что атрибута t у директории /tmp нет: Повторите предыдущие шаги [@fig:15]



```
[guest2@yupopova ~]$ su -
Password:
su: Authentication failure
[guest2@yupopova ~]$ su -
Password:
[root@yupopova ~]# chmod -t /tmp
[root@yupopova ~]# exit
logout
[guest2@yupopova ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 Oct  8 09:34 tmp
[guest2@yupopova ~]$ cat /tmp/file01.txt
test3
[guest2@yupopova ~]$ echo "test3" > /tmp/file01.txt
[guest2@yupopova ~]$ cat /tmp/file01.txt
test3
[guest2@yupopova ~]$ rm /tmp/file01.txt
[guest2@yupopova ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
[guest2@yupopova ~]$ chmod -t /tmp
```

{#fig:15 width=100%}

Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp [@fig:16]



```
[root@yupopova ~]# chmod +t /tmp
[root@yupopova ~]# exit
logout
[guest@yupopova lab5]$
```

{#fig:16 width=100%}

Выводы

В результате выполнения работы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получили практические навыки работы в консоли с дополнительными атрибутами, а также рассмотрели работы механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.

Список литературы

1. Методические материалы курса