

Информационная безопасность.

Лабораторная работа №5.

Филиппова Вероника Сергеевна.

Содержание

Цель работы	1
Задание	1
Выполнение лабораторной работы	1
Создание программы.....	1
Исследование Sticky-бита.....	7
Выводы	8

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

Задание

- 1) Создание программы.
- 2) Исследование Sticky-бита

Выполнение лабораторной работы

Создание программы

Проверила версию gcc с помощью программы gcc -v

```
vsfilippova@vsfilippova:~  
Файл Правка Вид Поиск Терминал Справка  
[vsfilippova@vsfilippova ~]$ gcc -v  
Используются внутренние спецификации.  
COLLECT_GCC=gcc  
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/4.8.5/lto-wrapper  
Целевая архитектура: x86_64-redhat-linux  
Параметры конфигурации: ../configure --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --  
-with-bugurl=http://bugzilla.redhat.com/bugzilla --enable-bootstrap --enable-shared --enable-threads=p  
osix --enable-checking=release --with-system-zlib --enable-__cxa_atexit --disable-libunwind-exceptions  
--enable-gnu-unique-object --enable-linker-build-id --with-linker-hash-style=gnu --enable-languages=c  
,c++,objc,obj-c++,java,fortran,ada,go,lto --enable-plugin --enable-initfini-array --disable-libgcj --w  
ith-isl=/build/builddir/build/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/isl-install --with-cloog=/bui  
lldir/build/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/cloog-install --enable-gnu-indirect-funct  
ion --with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux  
Модель многопоточности: posix  
gcc версия 4.8.5 20150623 (Red Hat 4.8.5-44) (GCC)  
[vsfilippova@vsfilippova ~]$
```

Рисунок 1

Отменила на текущую сессию SELinux командой `setenforce 0` Вошла в систему от имени пользователя `guest`, создала программу `simpleid.c`

```
[guest@vsfilippova vsfilippova]$ su --  
Пароль:  
[root@vsfilippova vsfilippova]# setenforce 0  
[root@vsfilippova vsfilippova]# getenforce  
Permissive  
[root@vsfilippova vsfilippova]# su - guest  
Последний вход в систему: Сб ноя 13 14:10:52 MSK 2021 на pts/0  
[guest@vsfilippova ~]$ touch simpleid.c  
[guest@vsfilippova ~]$ gedit simpleid.c
```

Рисунок 2

Скомпилировала программу и убедилась, что файл программы создан, командой `gcc simpleid.c -o simpleid`

```
Открыть simpleid.c admin:///home/guest Сохранить  
#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@vsfilippova vsfilippova]# setenforce 0  
[root@vsfilippova vsfilippova]# getenforce  
Permissive  
[root@vsfilippova vsfilippova]# su - guest  
Последний вход в систему: Сб ноя 13 14:10:52 MSK 2021 на pts/0  
[guest@vsfilippova ~]$ touch simpleid.c  
[guest@vsfilippova ~]$ gedit simpleid.c  
  
(gedit:7730): Gtk-WARNING **: 14:13:48.793: cannot open display:  
[guest@vsfilippova ~]$ touch simpleid.c  
[guest@vsfilippova ~]$ gedit simpleid.c  
  
(gedit:7908): Gtk-WARNING **: 14:15:30.614: cannot open display:  
[guest@vsfilippova ~]$ gedit simpleid.c  
  
(gedit:7930): Gtk-WARNING **: 14:16:11.105: cannot open display:  
[guest@vsfilippova ~]$ gcc simpleid.c -o simpleid  
[guest@vsfilippova ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@vsfilippova ~]$
```

Рисунок 3

Выполнила программу `simpleid`: `./simpleid` и программу `id` и сравнила полученный результат с данными предыдущего пункта. Полученные значения `id` совпадают

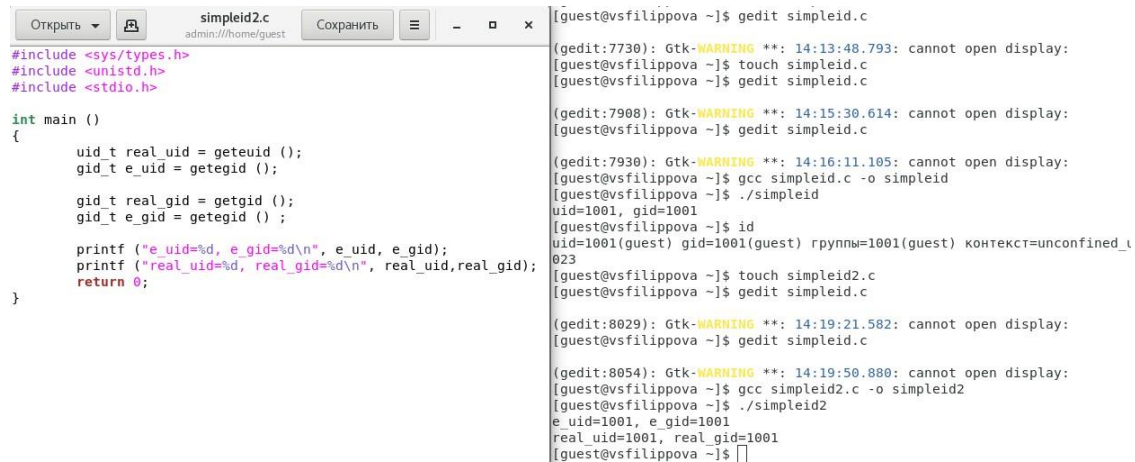
```

[guest@vsfilippova ~]$ ./simpleid
uid=1001, gid=1001
[guest@vsfilippova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1
023
[guest@vsfilippova ~]$

```

Рисунок 4

Усложнила программу, добавив вывод действительных идентификаторов, назвала программу simpleid2.c. Скомпилировала и запустила `simpleid2.c gcc simpleid2.c -o simpleid2`, а затем `./simpleid2`



```

[guest@vsfilippova ~]$ gedit simpleid.c
(gedit:7730): Gtk-WARNING **: 14:13:48.793: cannot open display:
[guest@vsfilippova ~]$ touch simpleid.c
[guest@vsfilippova ~]$ gedit simpleid.c
(gedit:7908): Gtk-WARNING **: 14:15:30.614: cannot open display:
[guest@vsfilippova ~]$ gedit simpleid.c
(gedit:7930): Gtk-WARNING **: 14:16:11.105: cannot open display:
[guest@vsfilippova ~]$ gcc simpleid.c -o simpleid
[guest@vsfilippova ~]$ ./simpleid
uid=1001, gid=1001
[guest@vsfilippova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1
023
[guest@vsfilippova ~]$ touch simpleid2.c
[guest@vsfilippova ~]$ gedit simpleid2.c
(gedit:8029): Gtk-WARNING **: 14:19:21.582: cannot open display:
[guest@vsfilippova ~]$ gedit simpleid2.c
(gedit:8054): Gtk-WARNING **: 14:19:50.880: cannot open display:
[guest@vsfilippova ~]$ gcc simpleid2.c -o simpleid2
[guest@vsfilippova ~]$ ./simpleid2
e uid=1001, e gid=1001
real uid=1001, real gid=1001
[guest@vsfilippova ~]$

```

Рисунок 5

От имени суперпользователя выполнила команды: `chown root:guest /home/guest/simpleid2` и `chmod u+s /home/guest/simpleid2`. Первая команда изменяет права на файл с guest на root. А затем устанавливает атрибут SetUID, который запускает программу не с правами пользователя, а с правами владельца файла. Затем выполнила проверку изменений с помощью команды `ls -l simpleid2`

```
guest@vsfilippova:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@vsfilippova ~]$ gedit simpleid.c

(gedit:8029): Gtk-WARNING **: 14:19:21.582: cannot open display:
[guest@vsfilippova ~]$ gedit simpleid.c

(gedit:8054): Gtk-WARNING **: 14:19:50.880: cannot open display:
[guest@vsfilippova ~]$ gcc simpleid2.c -o simpleid2
[guest@vsfilippova ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@vsfilippova ~]$ su
Пароль:
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls
dirl simpleid simpleid2 simpleid2.c simpleid.c
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dirl
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dirl
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dirl
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]#
```

Рисунок 6

Запустила ./simpleid2, id. При данном запуске выводы совпадают.

```
guest@vsfilippova:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@vsfilippova ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@vsfilippova ~]$ su
Пароль:
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls
dir1 simpleid simpleid2 simpleid2.c simpleid.c
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwxrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
[root@vsfilippova guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@vsfilippova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsfilippova guest]#
```

Рисунок 7

Проделала то же самое с атрибутом SetGID (установление прав для владеющей группы).

Запустила файл. Теперь выводы для группы различны.

```
guest@vsfilippova:/home/guest
Файл Правка Вид Поиск Терминал Справка
dir1 simpleid simpleid2 simpleid2.c simpleid.c
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwxrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
[root@vsfilippova guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@vsfilippova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsfilippova guest]# chmod g+s simpleid2
[root@vsfilippova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
[root@vsfilippova guest]# ./simpleid2
e_uid=1001, e_gid=1001
real_uid=0, real_gid=0
[root@vsfilippova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsfilippova guest]#
```

Рисунок 8

Создала программу readfile.c

Откомпилировала программу: gcc readfile.c -o readfile

```
Открыть readfile.c Сохранить
#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[10];
    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;
}

Файл Правка Вид Поиск Терминал Справка
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chown root:guest /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# chmod u+s /home/guest/simpleid2
[root@vsfilippova guest]# ls -l
итого 32
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
[root@vsfilippova guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@vsfilippova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsfilippova guest]# chmod g+s simpleid2
[root@vsfilippova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
[root@vsfilippova guest]# ./simpleid2
e_uid=1001, e_gid=1001
real_uid=0, real_gid=0
[root@vsfilippova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsfilippova guest]# touch readfile.c
[root@vsfilippova guest]# gedit readfile.c
C Шрифта табуляции 8 Стр 21, Стб 16 ВСТ
(gedit:8300): Gtk-WARNING **: 14:29:25.049: cannot open display:
[root@vsfilippova guest]# gcc readfile.c -o readfile
```

Рисунок 9

Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь(root) мог прочитать его.

Проверила, что пользователь guest не может прочитать файл readfile.c

```

DG_DATA_DIRS=/home/guest/.local/share/flatpak/exports/Ошибка сегментирования (core dumped)
[root@vsfilippova guest]# ls -l
итого 48
drwxrwxr-x. 2 guest guest 19 окт 30 11:21 dir1
-rwxr-xr-x. 1 root guest 8640 ноя 13 14:32 readfile
-rw-r--r-. 1 root root 417 ноя 13 14:32 readfile.c
-rwxrwxr-x. 1 guest guest 8592 ноя 13 14:17 simpleid
-rwsrwsr-x. 1 root guest 8648 ноя 13 14:21 simpleid2
-rw-rw-rw-. 1 guest guest 313 ноя 13 14:21 simpleid2.c
-rwxrwxrwx. 1 guest guest 180 ноя 13 14:17 simpleid.c
[root@vsfilippova guest]# ls -l readfile
-rwxr-xr-x. 1 root guest 8640 ноя 13 14:32 readfile
[root@vsfilippova guest]# chmod 700 readfile.c
[root@vsfilippova guest]# exit
exit
[guest@vsfilippova ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@vsfilippova ~]$
```

Рисунок 10

Сменила у программы readfile владельца и установила SetU'D-бит.

Проверила, может ли программа readfile прочитать файл readfile.c. Да.

Проверила, может ли программа readfile прочитать файл /etc/shadow. Да.

```

[root@vsfilippova guest]# exit
exit
[guest@vsfilippova ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@vsfilippova ~]$ chmod u+s /home/guest/readfile
chmod: изменение прав доступа для «/home/guest/readfile»: Операция не позволена
[guest@vsfilippova ~]$ su
Пароль:
[root@vsfilippova guest]# chown root:guest /home/guest/readfile.c
[root@vsfilippova guest]#
```

Рисунок 11

Исследование Sticky-бита.

Узнала, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду
ls -l / | grep tmp

От имени пользователя guest создала файл file01.txt в директории /tmp со словом test
echo "test" > /tmp/file01.txt

```

[guest@vsfilippova ~]$ ls -l / | grep tmp
drwxrwxrwt. 29 root root 4096 ноя 13 14:41 tmp
[guest@vsfilippova ~]$ echo

[guest@vsfilippova ~]$ "test"
[guest@vsfilippova ~]$ echo "test" > /tmp/file01.txt
[guest@vsfilippova ~]$ ls -l /tmp/file01.txt
ls: невозможно получить доступ к /tmp/file01.txt: Нет такого файла или каталога
[guest@vsfilippova ~]$
```

Рисунок 12

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

1. `ls -l /tmp/file01.txt,`
2. `chmod o+rw /tmp/file01.txt,`
3. `ls -l /tmp/file01.txt`

```
[guest@vsfilippova ~]$ "test"
[guest@vsfilippova ~]$ echo "test" > /tmp/file01.txt
[guest@vsfilippova ~]$ ls -l /tmp/file01.txt
ls: невозможно получить доступ к /tmp/file01.txt: Нет такого файла или каталога
[guest@vsfilippova ~]$ echo "test" > /tmp/file01.txt
[guest@vsfilippova ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 13 14:45 /tmp/file01.txt
[guest@vsfilippova ~]$ chmod o+rw /tmp/file01.txt
[guest@vsfilippova ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ноя 13 14:45 /tmp/file01.txt
[guest@vsfilippova ~]$
```

Рисунок 13

От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt: `cat /tmp/file01.txt`

Попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt`

Попробовала дозаписать в файл /tmp/file01.txt слово test2 командой `echo "test2" >> /tmp/file01.txt`

Проверила содержимое файла командой `cat /tmp/file01.txt`

[Рисунок 14](../scr/13.png{ #fig:014 width=70% }

От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt` Файл удалить не удалось.

[Рисунок 15](../scr/14.png{ #fig:015 width=70% }

Повысила свои права до суперпользователя командой `su -` и выполнила после этого команду, снимающую атрибут `t` (Sticky-бит) с директории /tmp: `chmod -t /tmp`

[Рисунок 16](../scr/16.png{ #fig:016 width=70% }

Повысила свои права до суперпользователя и вернула атрибут `t` на директорию /tmp: `su -, chmod +t /tmp, exit`

[Рисунок 17](../scr/17.png{ #fig:015 width=70% }

Выводы

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