

Отчёт по лабораторной работе №5

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Создание программы	6
2.2	Исследование Sticky-бита	10
3	Выводы	13

Список иллюстраций

2.1	Программа simpleid.c	6
2.2	Выполнение программы	7
2.3	Программа simpleid2.c	7
2.4	Компиляция и запуск	8
2.5	Изменение атрибутов, запуск	8
2.6	Программа readfile.c	9
2.7	Компиляция программы, смена прав доступа	9
2.8	Установка SetU'D-бита, проверка	10
2.9	Файл /etc/shadow	10
2.10	Проверка атрибута, работа с файлом	11
2.11	Действия с файлом от другого пользователя	11
2.12	Действия с файлом от другого пользователя	11
2.13	Снятие Sticky-бита с директории	12
2.14	Запись, чтение и удаление	12
2.15	Возвращение атрибута t	12

Список таблиц

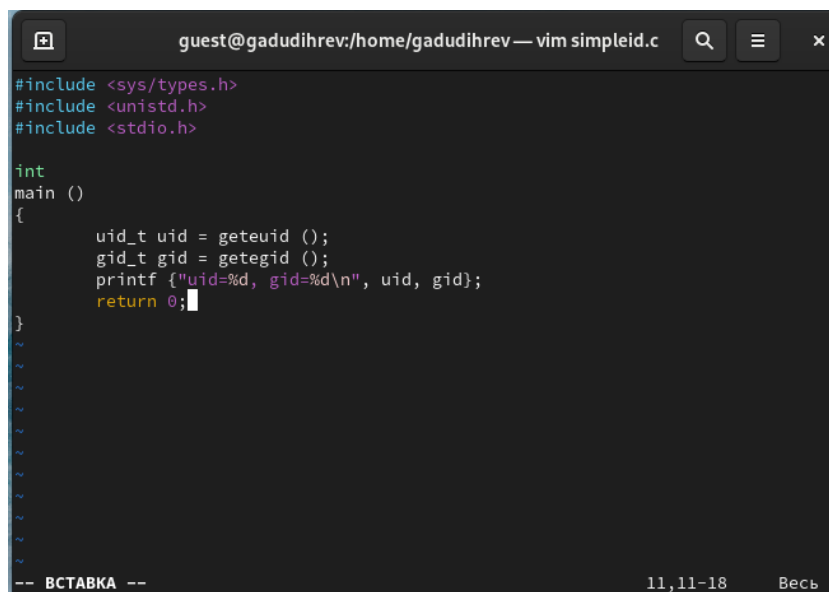
1 Цель работы

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.

2 Выполнение лабораторной работы

2.1 Создание программы

1. Создаю файл simpleid.c (рис. 2.1)



```
guest@gadudihrev:/home/gadudihrev — vim 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;
}
~
~
~
~
~
~
~
~
~
~
-- ВСТАВКА -- 11,11-18 Весь
```

Рис. 2.1: Программа simpleid.c

2. Компилирую программу командой `gcc simpleid.c -o simpleid` и проверяю, что файл создан. Выполняю программу simpleid командой `./simpleid`, а затем системную программу `id` - вывод одинаков. (рис. 2.2)

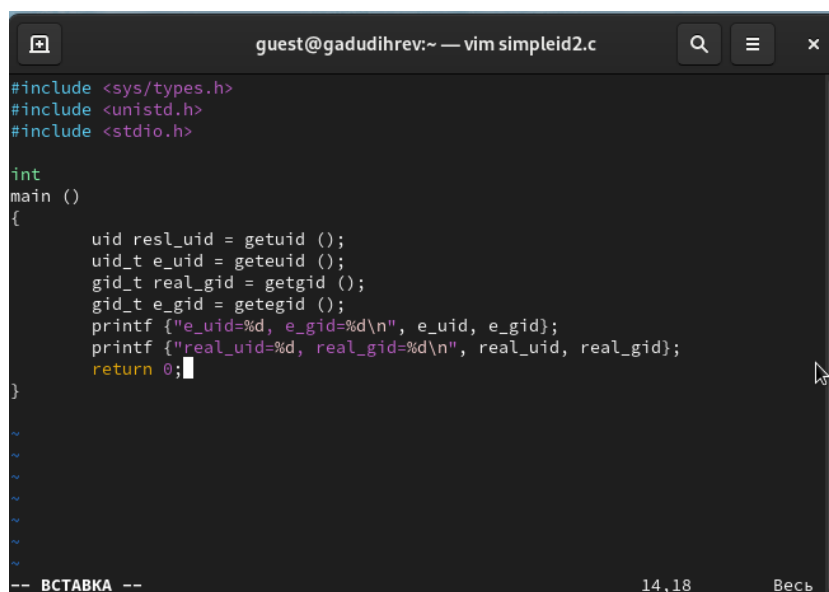
```

[guest@gadudihrev ~]$ vim simpleid.c
[guest@gadudihrev ~]$ gcc simpleid.c -0 simpleid
gcc: ошибка: unrecognized command-line option «-0»
[guest@gadudihrev ~]$ gcc simpleid.c -o simpleid
simpleid.c: В функции «main»:
simpleid.c:10:15: ошибка: expected «;» before «{» token
   10 |         printf ("uid=%d, gid=%d\n", uid, gid);
       |               ^
[guest@gadudihrev ~]$ vim simpleid.c
[guest@gadudihrev ~]$ gcc simpleid.c -o simpleid
simpleid.c: В функции «main»:
simpleid.c:10:46: ошибка: expected «;» before «return»
   10 |         printf ("uid=%d, gid=%d\n", uid, gid)
       |                                              ^
   11 |         return 0;
       |         ^
[guest@gadudihrev ~]$ vim simpleid.c
[guest@gadudihrev ~]$ gcc simpleid.c -o simpleid
[guest@gadudihrev ~]$ ./simpleid
uid=1001, gid=1001
[guest@gadudihrev ~]$

```

Рис. 2.2: Выполнение программы

3. Усложняю программу и записываю ее в файл simpleid2.c (рис. 2.3)



```

guest@gadudihrev:~ — vim simpleid2.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t resl_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;
}
-- ВСТАВКА --
14,18
Весь

```

Рис. 2.3: Программа simpleid2.c

4. Компилирую и запускаю программу командами `gcc simpleid2.c -o simpleid2` и `./simpleid2` (рис. 2.4)

```
guest@gadudihrev:~  
[guest@gadudihrev ~]$ vim simpleid2.c  
[guest@gadudihrev ~]$ gcc simpleid2.c -o simpleid2  
[guest@gadudihrev ~]$ ./simpleid2.o  
bash: ./simpleid2.o: Нет такого файла или каталога  
[guest@gadudihrev ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@gadudihrev ~]$
```

Рис. 2.4: Компиляция и запуск

5. От суперпользователя выполняю команды `chown root:guest /home/guest/simpleid2` и `chmod u+s /home/guest/simpleid2`. Проверяю правильность новых атрибутов командой `ls -l simpleid2`. Запускаю `simpleid2` и `id: ./simpleid2, id` (рис. 2.5)

```
[guest@gadudihrev ~]$ su  
Пароль:  
[root@gadudihrev guest]# chown root:guest /home/guest/simpleid2  
[root@gadudihrev guest]# chmod u+s /home/guest/simpleid2  
[root@gadudihrev guest]# ls -l simpleid2  
-rwsr-xr-x. 1 root guest 24488 anp 13 20:23 simpleid2  
[root@gadudihrev guest]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@gadudihrev guest]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@gadudihrev guest]#
```

Рис. 2.5: Изменение атрибутов, запуск

6. Создаю программу `readfile.c` (рис. 2.6)

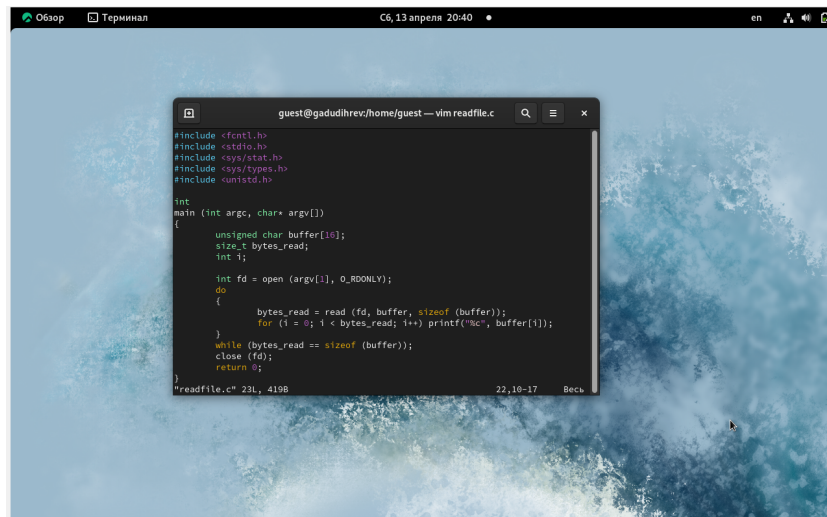


Рис. 2.6: Программа readfile.c

7. Компилирую ее командой `gcc readfile.c -o readfile` и изменяю права доступа так, чтобы только суперпользователь мог прочитать его, а guest не мог (рис. 2.7)

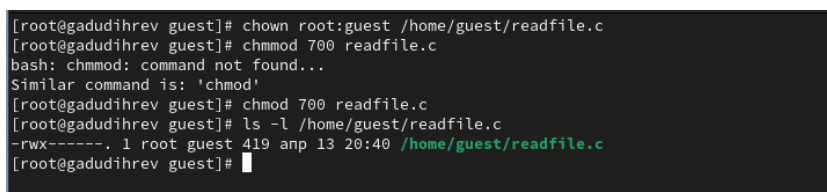


Рис. 2.7: Компиляция программы, смена прав доступа

8. Командой `cat readfile.c` проверяю, что пользователь guest не может прочитать файл readfile.c. Устанавливаю SetU'D-бит и теперь от пользователя guest можно прочитать файл (рис. 2.8)

```

[root@gadudihrev guest]# su guest
[guest@gadudihrev ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@gadudihrev ~]$ su
Пароль:
[root@gadudihrev guest]# chmod u+s /home/guest/readfile.c
[root@gadudihrev guest]# readfile readfile.c
bash: readfile: command not found...
[root@gadudihrev guest]# ./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;
}
[root@gadudihrev guest]#

```

Рис. 2.8: Установка SetU'D-бита, проверка

9. Проверяю, может ли программа readfile прочитать файл /etc/shadow - да, может (рис. 2.9)

```

[root@gadudihrev guest]# ./readfile /etc/shadow
root:$6$1WRz..Hl4hg8YS8$zUdYL1JycC8MK.4/FohMXML8bCUa0NSLwBzMoxXk6l.upogud82tHucQrgRI/AtUox16N6QRna4R6F9LjKw20:0:99999
:7:::
bin:!:19469:0:99999:7:::
daemon:!:19469:0:99999:7:::
adm:!:19469:0:99999:7:::
lp:!:19469:0:99999:7:::
sync:!:19469:0:99999:7:::
shutdown:!:19469:0:99999:7:::
halt:!:19469:0:99999:7:::
mail:!:19469:0:99999:7:::
operator:!:19469:0:99999:7:::
games:!:19469:0:99999:7:::
ftp:!:19469:0:99999:7:::
nobody:!:19469:0:99999:7:::
systemd-coredump:!:19811:!:!:!:
dbus:!:19811:!:!:!:
polkitd:!:19811:!:!:!:
avahi:!:19811:!:!:!:
rtkit:!:19811:!:!:!:

```

Рис. 2.9: Файл /etc/shadow

2.2 Исследование Sticky-бита

10. Проверяю, установлен ли атрибут Sticky на директории /tmp командой `ls -l | grep tmp`. От пользователя guest создаю файл со словом test командой `echo "test" > /tmp/file01.txt`. Просматриваю атрибуты у только что созданного файла и разрешаю чтение и запись для категории пользователей «все остальные» (рис. 2.10)

```
guest@gadudihrev:~  
[root@gadudihrev guest]# ls -l / | grep tmp  
drwxrwxrwt. 17 root root 4096 anp 13 20:46 tmp  
[root@gadudihrev guest]# su guest  
[guest@gadudihrev ~]$ 15233563  
bash: 15233563: command not found...  
[guest@gadudihrev ~]$ echo "test" > /tmp/file01.txt  
[guest@gadudihrev ~]$ ls -l /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 anp 13 20:52 /tmp/file01.txt  
[guest@gadudihrev ~]$ chmod o+rw /tmp/file01.txt  
[guest@gadudihrev ~]$ ls -l /tmp/file01.txt  
-rw-r--rw-. 1 guest guest 5 anp 13 20:52 /tmp/file01.txt  
[guest@gadudihrev ~]$
```

Рис. 2.10: Проверка атрибута, работа с файлом

11. От пользователя guest пробую прочитать файл командой `cat /tmp/file01.txt`, далее записываю в файл слово `test2` и вновь читаю его - текст файла изменен (рис. 2.11)

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

Рис. 2.11: Действия с файлом от другого пользователя

12. От пользователя guest2 пробую записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt` - операцию выполнить удалось. Просматриваю содержимое файла и пробую удалить его - удалить не удалось (рис. 2.12)

```
[guest2@gadudihrev guest]$ echo "test3" > /tmp/file01.txt  
[guest2@gadudihrev guest]$ cat /tmp/file01.txt  
test3  
[guest2@gadudihrev guest]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@gadudihrev guest]$
```

Рис. 2.12: Действия с файлом от другого пользователя

13. От суперпользователя ввожу команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`: `chmod -t /tmp`. Проверяю от пользователя guest2, что атрибута `t` у директории `/tmp` нет командой `ls -l / | grep tmp` (рис. 2.13)

```
[guest2@gadudihrev guest]$ su
Пароль:
[root@gadudihrev guest]# chmod -t /tmp
[root@gadudihrev guest]# exit
exit
[guest2@gadudihrev guest]$ ls -l | grep tmp
[guest2@gadudihrev guest]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 апр 13 21:05 tmp
[guest2@gadudihrev guest]$
```

Рис. 2.13: Снятие Sticky-бита с директории

14. Снова пробую записать, прочитать и удалить файл - все операции выполнены успешно (рис. 2.14)

```
[guest2@gadudihrev guest]$ cat /tmp/file01.txt
test3
[guest2@gadudihrev guest]$ echo "test4" > /tmp/file01.txt
[guest2@gadudihrev guest]$ cat /tmp/file01.txt
test4
[guest2@gadudihrev guest]$ rm /tmp/file01.txt
[guest2@gadudihrev guest]$
```

Рис. 2.14: Запись, чтение и удаление

15. Возвращаюсь в суперпользователя и возвращаю атрибут `t` на директорию `/tmp` командой `chmod +t /tmp` (рис. 2.15)

```
[guest2@gadudihrev guest]$ su
Пароль:
[root@gadudihrev guest]# chmod +t /tmp
[root@gadudihrev guest]# exit
exit
[guest2@gadudihrev guest]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 апр 13 21:07 tmp
[guest2@gadudihrev guest]$
```

Рис. 2.15: Возвращение атрибута `t`

3 Выводы

Я научился применять SetUID- и Sticky-биты, поработал с дополнительными атрибутами в консоли, рассмотрел работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.