

**Лабораторная работа № 5.
Дискреционное разграничение прав в
Linux. Исследование влияния
дополнительных атрибутов**

Лёшьен Стефани, НФИбд-02-19

Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6
3	Выводы	12
4	Выводы	13
5	Библиография	14

List of Figures

2.1	Установка gcc и создание файла simpleid.c	6
2.2	Код программы в simpleid.c	7
2.3	Скомпилировали и выполните программу simpleid	7
2.4	Код программы в simpleid2.c	8
2.5	Выполнили команды chown и chmod	8
2.6	программу readfile.c	9
2.7	Смените владельца у файла readfile.c	9
2.8	Изменили права	9
2.9	атрибут Sticky на директории /tmp	10
2.10	Разрешили чтение и запись для категории пользователей все остальные	11
2.11	Сняли атрибут Sticky и смогли удалить файл.	11

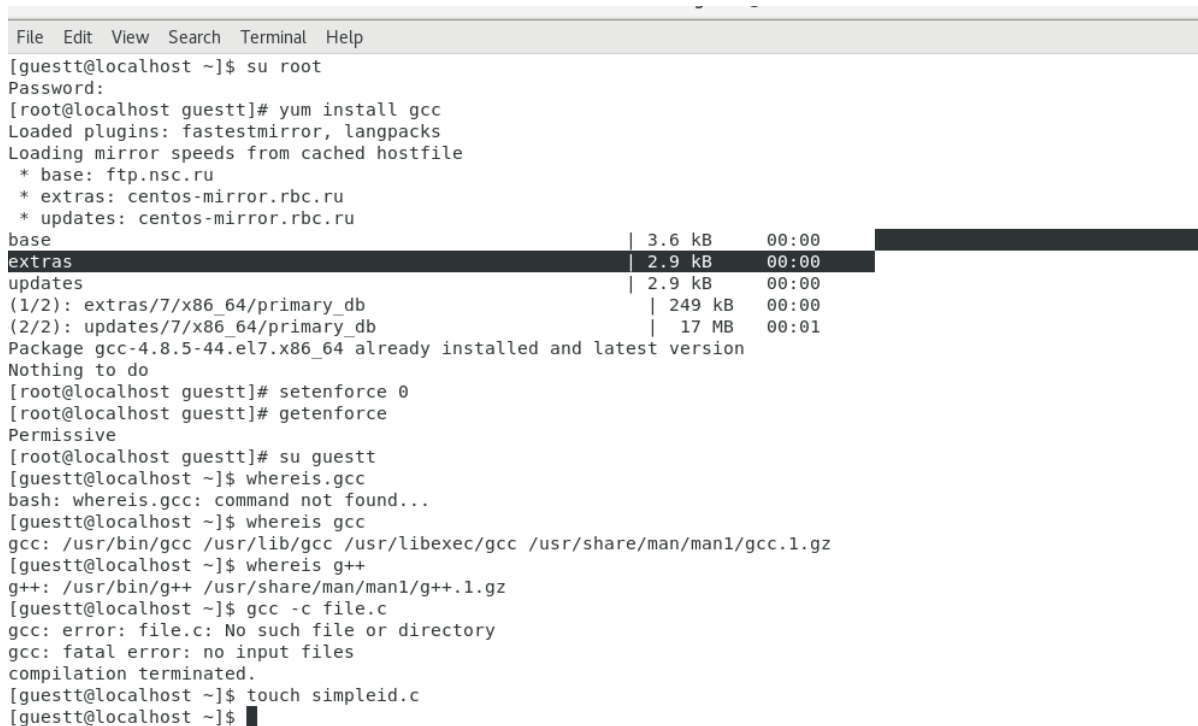
List of Tables

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.

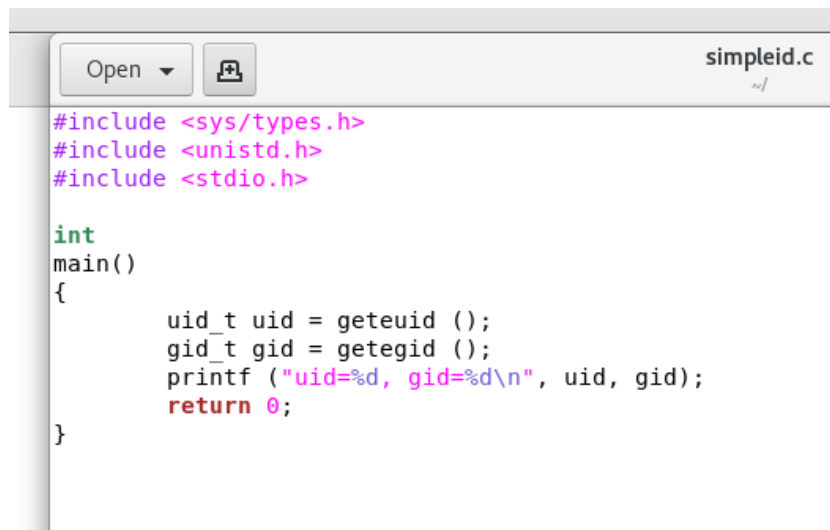
2 Последовательность выполнения работы

1. От имени пользователя root установили компилятор gcc с помощью команды `yum install gcc`.
2. Создали файл `simpleid.c`



```
File Edit View Search Terminal Help
[guesttt@localhost ~]$ su root
Password:
[root@localhost guesttt]# yum install gcc
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.nsc.ru
 * extras: centos-mirror.rbc.ru
 * updates: centos-mirror.rbc.ru
base | 3.6 kB | 00:00
extras | 2.9 kB | 00:00
updates | 2.9 kB | 00:00
(1/2): extras/7/x86_64/primary_db | 249 kB | 00:00
(2/2): updates/7/x86_64/primary_db | 17 MB | 00:01
Package gcc-4.8.5-44.el7.x86_64 already installed and latest version
Nothing to do
[root@localhost guesttt]# setenforce 0
[root@localhost guesttt]# getenforce
Permissive
[root@localhost guesttt]# su guesttt
[guesttt@localhost ~]$ whereis gcc
bash: whereis.gcc: command not found...
[guesttt@localhost ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz
[guesttt@localhost ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[guesttt@localhost ~]$ gcc -c file.c
gcc: error: file.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[guesttt@localhost ~]$ touch simpleid.c
[guesttt@localhost ~]$
```

Figure 2.1: Установка gcc и создание файла `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;
}
```

Figure 2.2: Код программы в simpleid.c

4. Скомпилировали программу и убедились, что файл программы создан.
5. Выполните программу simpleid и системную программу id.

```
[guestt@localhost ~]$ gcc simpleid.c -o simpleid
[guestt@localhost ~]$ ./simpleid
uid=1001, gid=1002
[guestt@localhost ~]$ id
uid=1001(guestt) gid=1002(guestt) groups=1002(guestt) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guestt@localhost ~]$ touch simpleid2.c
[guestt@localhost ~]$
```

Figure 2.3: Скомпилировали и выполните программу simpleid

6. Создали файл simpleid2.c. Усложнили программу, добавив вывод действительных идентификаторов.

```

1  #include <sys/types.h>
2  #include <unistd.h>
3  #include <stdio.h>
4
5  int
6  main()
7  {
8      uid_t real_uid = getuid ();
9      uid_t e_uid = getuid ();
10
11     gid_t real_gid = getgid ();
12     gid_t e_gid = getgid ();
13
14     printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
15     printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
16
17     return 0;
18 }

```

Figure 2.4: Код программы в simpleid2.c

7. Скомпилируйте и запустите simpleid2.c.
8. От имени суперпользователя выполните команды: `chown root:guest /home/guest/simpleid2` Эта команда изменяет права владения файла. Мы установили владения для root и группы guest. `chmod u+s /home/guest/simpleid2` Эта команда добавляет выполнение от имени пользователя для юзера.(рис. -fig. 2.5)
9. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2 с помощью `ls`.

```

[guestt@localhost ~]$ gcc simpleid.c -o simpleid
[guestt@localhost ~]$ ./simpleid
uid=1001, gid=1002
[guestt@localhost ~]$ id
uid=1001(guestt) gid=1002(guestt) groups=1002(guestt) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guestt@localhost ~]$ touch simpleid2.c
[guestt@localhost ~]$ gcc simpleid2.c -o simpleid2
[guestt@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1002
real_uid=1001, real_gid=1002
[guestt@localhost ~]$ id
uid=1001(guestt) gid=1002(guestt) groups=1002(guestt) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guestt@localhost ~]$ su root
Password:
[root@localhost guestt]# chown root:guest /home/guest/simpleid2
chown: cannot access '/home/guest/simpleid2': No such file or directory
[root@localhost guestt]# chown root:guestt /home/guestt/simpleid2
[root@localhost guestt]# chmod u+s /home/guestt/simpleid2
[root@localhost guestt]# ls -l simpleid2
-rwsrwxr-x. 1 root guestt 8464 Oct 7 03:09 simpleid2
[root@localhost guestt]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@localhost guestt]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost guestt]#

```

Figure 2.5: Выполнили команды chown и chmod

10. Создайте программу readfile.c и откомпилировали её.



```
#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;
}
```

Figure 2.6: программу readfile.c

11. Смените владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог. Проверили что пользователь guest не может прочитать файл readfile.c. В результате чего было отказано в чтение файла. (рис. -fig. 2.7)

```
[guestt@localhost ~]$ gcc readfile1.c -o readfile1
[guestt@localhost ~]$ su root
Password:
[root@localhost guestt]# chown root /home/guestt/readfile1.c
```

Figure 2.7: Смените владельца у файла readfile.c

```
[root@localhost guestt]# chmod 700 /home/guestt/readfile1.c
[root@localhost guestt]# sur guestt
bash: sur: command not found...
[root@localhost guestt]# su guest
su: user guest does not exist
[root@localhost guestt]# su guestt
[guestt@localhost ~]$ cat readfile1.c
cat: readfile1.c: Permission denied
[guestt@localhost ~]$ █
```

Figure 2.8: Изменили права

12. Выяснили, что атрибут Sticky установлен на директории /tmp, для чего выполните команду `ls -l / | grep tmp`.

```
[guestt@localhost home]$ ls -l / grep tmp
ls: cannot access grep: No such file or directory
ls: cannot access tmp: No such file or directory
/:
total 24
lrwxrwxrwx. 1 root root 7 Sep 23 07:21 bin -> usr/bin
dr-xr-xr-x. 5 root root 4096 Sep 23 07:53 boot
drwxr-xr-x. 20 root root 3200 Oct 7 02:38 dev
drwxr-xr-x. 140 root root 8192 Oct 7 02:48 etc
drwxr-xr-x. 5 root root 51 Sep 25 17:48 home
lrwxrwxrwx. 1 root root 7 Sep 23 07:21 lib -> usr/lib
lrwxrwxrwx. 1 root root 9 Sep 23 07:21 lib64 -> usr/lib64
drwxr-xr-x. 2 root root 6 Apr 11 2018 media
drwxr-xr-x. 2 root root 6 Apr 11 2018 mnt
drwxr-xr-x. 4 root root 49 Sep 23 07:42 opt
dr-xr-xr-x. 239 root root 0 Oct 7 02:38 proc
dr-xr-xr-x. 5 root root 265 Oct 7 03:17 root
drwxr-xr-x. 42 root root 1320 Oct 7 02:51 run
lrwxrwxrwx. 1 root root 8 Sep 23 07:21 sbin -> usr/sbin
drwxr-xr-x. 2 root root 6 Apr 11 2018 srv
dr-xr-xr-x. 13 root root 0 Oct 7 02:38 sys
drwxrwxrwt. 23 root root 4096 Oct 7 03:38 tmp
drwxr-xr-x. 13 root root 155 Sep 23 07:21 usr
drwxr-xr-x. 20 root root 282 Sep 23 07:37 var
[guestt@localhost home]$ ls -l / | grep tmp
drwxrwxrwt. 23 root root 4096 Oct 7 03:38 tmp
[guestt@localhost home]$
```

Figure 2.9: атрибут Sticky на директории /tmp

13. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные».
14. От пользователя guest2 (не являющегося владельцем) попробовали прочитать файл. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой `echo "test2" > /tmp/file01.txt`. Проверили содержимое файла. Попробовали удалить файл.

```

[guestt@localhost home]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guestt guestt 5 Oct  7 03:52 /tmp/file01.txt
[guestt@localhost home]$ chmod o+rw /tmp/file01.txt
[guestt@localhost home]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guestt guestt 5 Oct  7 03:52 /tmp/file01.txt
[guestt@localhost home]$ su guest2
Password:
[guest2@localhost home]$ cat /tmp/file01.txt
test
[guest2@localhost home]$ echo "test2" > /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01.txt
test2
[guest2@localhost home]$ echo "test3" > /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01.txt
test3
[guest2@localhost home]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted

```

Figure 2.10: Разрешили чтение и запись для категории пользователей все остальные

15. Повысили свои права до суперпользователя следующей командой `su -` и выполните после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`. Повторили предыдущие шаги. Нам теперь удалось удалить файл.

```

[guest2@localhost home]$ su -
Password:
Last login: Fri Oct  7 03:37:56 EDT 2022 on pts/0
Last failed login: Fri Oct  7 04:00:48 EDT 2022 on pts/0
There was 1 failed login attempt since the last successful login.
[root@localhost ~]# chmod -t /tmp
[root@localhost ~]# exit
logout
[guest2@localhost home]$ ls -l / | grep tmp
drwxrwxrwx. 23 root root 4096 Oct  7 04:00 tmp
[guest2@localhost home]$ cat /tmp/file01.txt
test3
[guest2@localhost home]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01
cat: /tmp/file01: No such file or directory
[guest2@localhost home]$ cat /tmp/file01.txt
test3
test2
[guest2@localhost home]$ echo "test3" > /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01.txt
test3
[guest2@localhost home]$ rm /tmp/file01.txt
[guest2@localhost home]$ su
Password:
[root@localhost home]# chmod +t /tmp
[root@localhost home]# exit
exit
[guest2@localhost home]$ █

```

Figure 2.11: Сняли атрибут Sticky и смогли удалить файл.

3 Выводы

Изучили механизмов изменения идентификаторов, применения SetUID- и Sticky-битов.

4 Выводы

Получили практических навыков работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

5 Библиография

1. Методические материалы курса