

Информационная безопасность.

Лабораторная работа #5.

**Дискреционное разграничение прав в Linux. Исследование влияния
дополнительных атрибутов**

Хохлачева Яна, учебная группа: НКНбд-01-18

Содержание

0.1	Цель работы	3
1	Создание программы	4
2	Исследование Sticky-бита	10
2.1	Вывод	12

Список иллюстраций

1.1	Выполнение simpleid.c и команды id	5
1.2	Запуск simpleid2.c	6
1.3	Установка новых атрибутов и смены владельца файла	6
1.4	Проверка правильности	6
1.5	simpleid2 и id	7

0.1 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.

1 Создание программы

1. Подготовила стенд лабораторной в соответствии с указаниями, а в частности:

- Проверила наличие компилятора GCC командой: **gcc -v**
- Отключила систему запретов до очередной перезагрузки системы командой **setenforce 0** и проверила вывод кодады **getenforce**
- Ознакомилась с информацией о компиляции программ при помощи GCC.

2. Вошла в систему от имени пользователя **guest**.

3. Создала программу **simpleid.c** со следующим содержанием:

```
#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;
}
```

4. Скомпилировала программу при помощи команды **gcc simpleid.c -o simpleid** и убедилась, что файл программы создан.

5. Выполнила программу **simpleid** командой **./simpleid**.
6. Выполнила системную команду **id**, результаты выполнения программы и команды - идентичные.

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

Рис. 1.1: Выполнение simpleid.c и команды id

7. Усложнила программу, добавив вывод действительных идентификаторов, назвала ее **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;
}
```

8. Скомпилировала и запустила **simpleid2.c** командами: **gcc simpleid2.c -o simpleid2**,
**** ./simpleid2****.

```
[guest@localhost ~]$ touch simpleid2.c
[guest@localhost ~]$ gedit simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 1.2: Запуск simpleid2.c

9. От имени суперпользователя выполнила команды: **chown root:guest /simpleid2**, **** chmod u+s /simpleid2**** .

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

Рис. 1.3: Установка новых атрибутов и смены владельца файла

10. Выполнила проверку правильности установки новых атрибутов и смены владельца файла **simpleid2** командой: **ls -l simpleid2**

```
[root@localhost guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 Nov 13 14:13 simpleid2
[root@localhost guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 1.4: Проверка правильности

11. Запустила **simpleid2** и **id**.

```
[guest@localhost ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 1.5: simpleid2 и id

Результаты отличаются

12. Прodelала тоже самое относительно SetGID-бита.

```
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chmod u-s /home/guest/simpleid2
[root@localhost guest]# chmod g+s /home/guest/simpleid2
bash: chmod: command not found...
Similar command is: 'chmod'
[root@localhost guest]# chmod g+s /home/guest/simpleid2
[root@localhost guest]# exit
exit
[guest@localhost ~]$ ls -l simpleid2
-rwxrwsr-x. 1 root guest 17648 Nov 13 14:13 simpleid2
```

13. Создала программу **readfile.c**:

```
[guest@localhost ~]$ touch readfile.c
[guest@localhost ~]$ gedit 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;
}

```

14. Откомпилировала её командой **gcc readfile.c -o readfile** и сменила владельца у файла **readfile.c** и изменила права так, чтобы только суперпользователь(root) мог прочитать его, а guest не мог, также проверила, что пользователь guest не может прочитать файл **readfile.c**.

```

[guest@localhost ~]$ gcc readfile.c -o readfile
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chown root:guest /home/guest/readfile.c
[root@localhost guest]# chmod 700 /home/guest/readfile.c
[root@localhost guest]# exit
exit
[guest@localhost ~]$ ls -l readfile.c
-rwx-----. 1 root guest 414 Nov 13 15:19 readfile.c

```

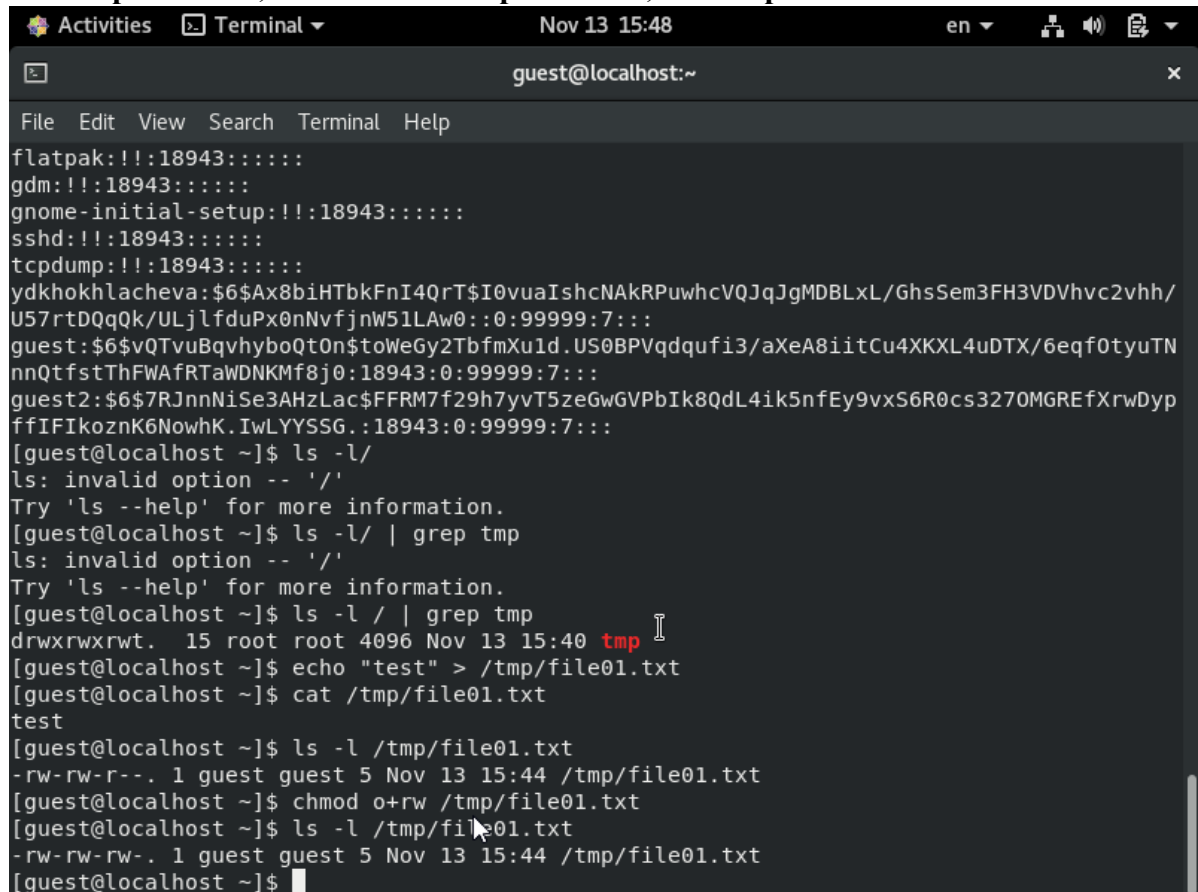
15. Сменила у программы **readfile** владельца и установила SetU'D-бит. Проверила, может ли программа **readfile** прочитать файл **readfile.c**. Проверила, что программа **readfile** прочитать файл **/etc/shadow**.


```
[guest@localhost ~]$ ls -l readfile.c
-rwx-----. 1 root guest 414 Nov 13 15:19 readfile.c
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chown root:guest /home/guest/readfile
[root@localhost guest]# chmod u+s /home/guest/readfile
[root@localhost guest]# exit
exit
[guest@localhost ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
```

2 Исследование Sticky-бита

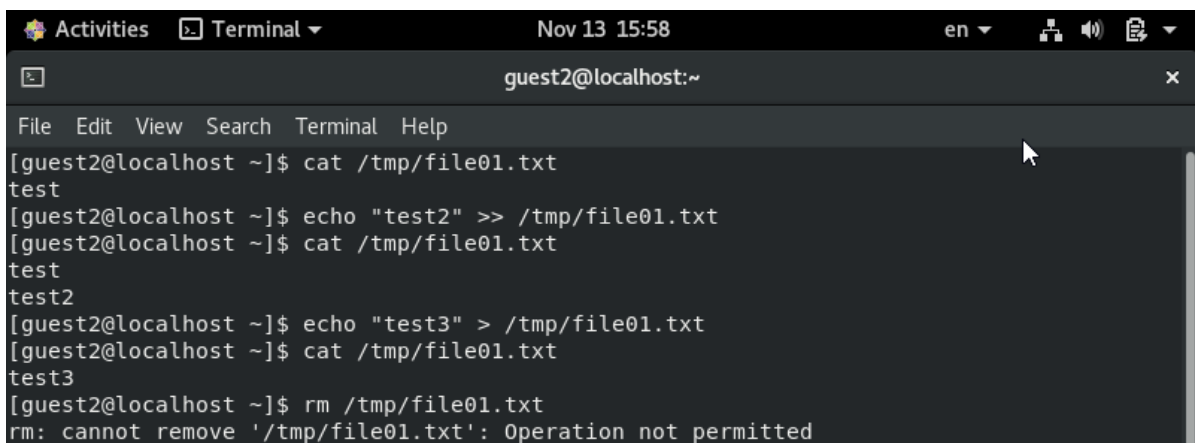
1. Выяснила, установлен ли атрибут Sticky на директории **/tmp**, для чего выполнил команду: **ls -l / | grep tmp**. От имени пользователя **guest** создала файл **file01.txt** в директории **/tmp** со словом **test** командой: **echo "test" > /tmp/file01.txt**. Просмотрела атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» командами:

ls -l /tmp/file01.txt, chmod o+rw /tmp/file01.txt, ls -l /tmp/file01.txt.



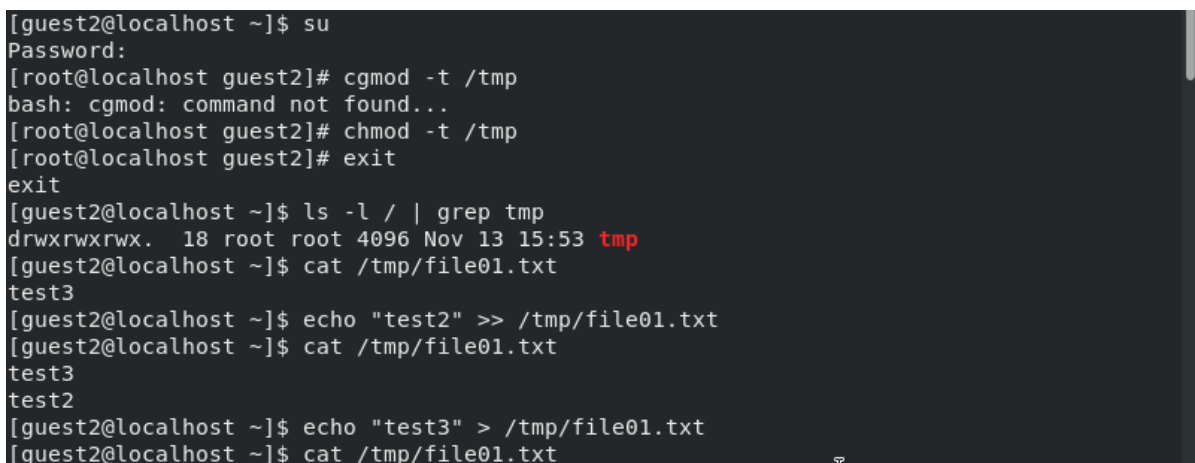
```
Activities Terminal Nov 13 15:48 en
guest@localhost:~
File Edit View Search Terminal Help
flatpak:!!:18943:~:
gdm:!!:18943:~:
gnome-initial-setup:!!:18943:~:
sshd:!!:18943:~:
tcpdump:!!:18943:~:
ydkhokhlacheva:$6$Ax8biHTbkFnI4QrT$I0vuaIshcNAkRPuwhcVQJqJgMDBLxL/GhsSem3FH3VDVhvc2vhh/
U57rtDQqQk/ULjlfduPx0nNvfjnW51LAw0::0:99999:7::
guest:$6$VQtvuBqvhyboQt0n$toWeGy2TbfmXuId.US0BPVqdqufi3/aXeA8iitCu4XKXL4uDTX/6eqf0tyuTN
nnQtfstThFWAfRTaWDNKMf8j0:18943:0:99999:7::
guest2:$6$7RJnnNiSe3AHzLac$FFRM7f29h7yvT5zeGwGVPbIk8QdL4ik5nfEy9vxS6R0cs3270MGREfXrwDyp
ffIFIKoznK6NowhK.IwLYYSSG.:18943:0:99999:7::
[guest@localhost ~]$ ls -l/
ls: invalid option -- '/'
Try 'ls --help' for more information.
[guest@localhost ~]$ ls -l/ | grep tmp
ls: invalid option -- '/'
Try 'ls --help' for more information.
[guest@localhost ~]$ ls -l / | grep tmp
drwxrwxrwt. 15 root root 4096 Nov 13 15:40 tmp
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
[guest@localhost ~]$ cat /tmp/file01.txt
test
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Nov 13 15:44 /tmp/file01.txt
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Nov 13 15:44 /tmp/file01.txt
[guest@localhost ~]$
```

2. От пользователя `guest2` попробовала прочитать файл `/tmp/file01.txt` командой: `cat /tmp/file01.txt`. От пользователя `guest2` попробовала дозаписать в файл `/tmp/file01.txt` слово `test2` командой `echo "test2" >> /tmp/file01.txt`. Удалось ли вам выполнить операцию? (Да). Проверила содержимое файла командой `cat /tmp/file01.txt`. От пользователя `guest2` попробовала записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt`. Удалось ли вам выполнить операцию? (Да). Проверила содержимое файла командой `cat /tmp/file01.txt`. От пользователя `guest2` попробовал удалить файл `/tmp/file01.txt` командой `rm /tmp/file01.txt`. Удалось ли вам удалить файл? (Нет)



```
Activities Terminal Nov 13 15:58 en
guest2@localhost:~
File Edit View Search Terminal Help
[guest2@localhost ~]$ cat /tmp/file01.txt
test
[guest2@localhost ~]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
test
test2
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
test3
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

3. Повысила свои права до суперпользователя следующей командой: `su -` И выполнила после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`: `chmod -t /tmp`. Покинула режим суперпользователя командой `exit`.



```
[guest2@localhost ~]$ su
Password:
[root@localhost guest2]# chmod -t /tmp
bash: chmod: command not found...
[root@localhost guest2]# chmod -t /tmp
[root@localhost guest2]# exit
exit
[guest2@localhost ~]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 Nov 13 15:53 tmp
[guest2@localhost ~]$ cat /tmp/file01.txt
test3
[guest2@localhost ~]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
test3
test2
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
```

4. От пользователя `guest2` проверил, что атрибута `t` у директории `/tmp` нет командой: `ls -l / | grep tmp`. Проверила предыдущие шаги. Удалось удалить файл от имени пользователя, не являющегося его владельцем

```
[guest2@localhost ~]$ cat /tmp/file01.txt
test3
[guest2@localhost ~]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
test3
test2
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt
[guest2@localhost ~]$ cat /tmp/file01.txt
```

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

```
[guest2@localhost ~]$ su
Password:
lsu: Authentication failure
[guest2@localhost ~]$ su
Password:
[root@localhost guest2]# chmod +t /tmp
[root@localhost guest2]# ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Nov 13 15:57 tmp
[root@localhost guest2]# exit
exit
[guest2@localhost ~]$
```

2.1 Вывод

- Изучила механизмы изменения идентификаторов, научилась применять SetUID- и Sticky-биты. 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.