

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Голощапова Ирина Борисовна

7 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Голощапова Ирина Борисовна
- студентка уч. группы НФИбд-01-20
- Российский университет дружбы народов
- 1032201666@pfur.ru
- <https://github.com/ibgoloshchapowa>

Вводная часть

Логические объекты файловой системы (файлы) являются носителями своеобразных меток, которые привычно называют правами доступа. Некоторые метки действительно означают право выполнения определенного действия пользователя над этим объектом. Важно изучить их для дальнейшего применения на практике.

- Атрибуты файлов
- Дистрибутив Rocky
- Дискреционное разграничение доступа

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.

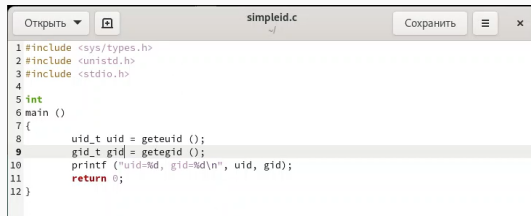
Выполнение работы

1. С правами администратора установила компилятор gcc

```
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# yum install gcc
packages for the GitHub CLI          11 kB/s | 3.0 kB   00:00
packages for the GitHub CLI          3.5 kB/s | 2.6 kB   00:00
Rocky Linux 9 - BaseOS               3.5 kB/s | 4.1 kB   00:01
Rocky Linux 9 - BaseOS              989 kB/s | 1.9 MB   00:01
Rocky Linux 9 - AppStream            5.4 kB/s | 4.5 kB   00:00
Rocky Linux 9 - AppStream           2.6 MB/s | 7.1 MB   00:02
Rocky Linux 9 - Extras               2.6 kB/s | 2.9 kB   00:01
Rocky Linux 9 - Extras              9.7 kB/s | 11 kB    00:01
Пакет gcc-11.3.1-4.3.el9.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@ibgoloshchapowa guest]#
```

Рис. 1: Установка gcc

2. Вошла в систему от имени пользователя guest и создала программу simpleid.c со следующим кодом



```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t uid = geteuid ();
9     gid_t gid = getegid ();
10    printf ("uid=%d, gid=%d\n", uid, gid);
11    return 0;
12 }
```

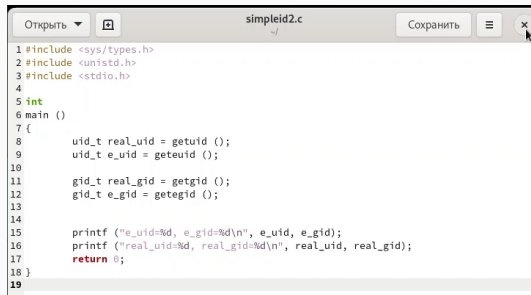
Рис. 2: simpleid.c

3. Скомпилировала программу и убедилась, что файл программы создан. Далее выполнила программу `simpleid` и системную программу `id`, сравнив полученный результат

```
[guest@ibgoloshchapowa ~]$ gcc simpleid.c -o simpleid
[guest@ibgoloshchapowa ~]$ ./simpleid
uid=1001, gid=1001
[guest@ibgoloshchapowa ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ibgoloshchapowa ~]$
```

Рис. 3: Выполнение программы `simpleid`

4. Усложнила 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 = geteuid ();
10
11     gid_t real_gid = getgid ();
12     gid_t e_gid = getegid ();
13
14
15     printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
16     printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
17     return 0;
18 }
19
```

Рис. 4: simpleid2.c

5. Скомпилировала и запустила simpleid2.c

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

Рис. 5: Запуск программы simpleid2.c

6. От имени суперпользователя выполнила команды, выполнила проверку правильности установки новых атрибутов и смены владельца файла `simpleid2` и запустила `simpleid2` и `id`:

```
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# chown root:guest /home/guest/simpleid2
[root@ibgoloshchapowa guest]# chmod u+s /home/guest/simpleid2
[root@ibgoloshchapowa guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 окт  5 21:26 simpleid2
[root@ibgoloshchapowa guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@ibgoloshchapowa guest]# id
uid=0(root) gid=0(root) rpyнны=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s
0:c0.c1023
[root@ibgoloshchapowa guest]#
```

Рис. 6: Установка новых атрибутов и смена владельца `simpleid2.c`

7. Создала программу readfile.c



```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 #include <fcntl.h>
6 #include <sys/stat.h>
7
8 int
9 main (int argc, char* argv[])
10 {
11     unsigned char buffer[10];
12     size_t bytes_read;
13     int i;
14
15     int fd = open (argv[1], O_RDONLY);
16     do
17     {
18         bytes_read = read (fd, buffer, sizeof (buffer));
19         for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
20     }
21     while (bytes_read == sizeof (buffer));
22     close (fd);
23     return 0;
24 }
```

Рис. 7: readfile.c

8. Откомпилировала программу. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь мог прочитать его, а guest не мог

```
[guest@ibgoloshchapowa ~]$ gcc readfile.c -o readfile
[guest@ibgoloshchapowa ~]$ su root
#
[root@ibgoloshchapowa guest]# chown root /home/guest/readfile
[root@ibgoloshchapowa guest]# chmod 700 /home/guest/readfile
[root@ibgoloshchapowa guest]# cat /home/guest/readfile
so.6GLIBC_2.34GLIBC_2.2.5_ITM_deregisterTMCloneTable__geon_start__ITM_r
cat: /home/guest/readfile: Отказано в доступе
[guest@ibgoloshchapowa ~]$
```

Рис. 8: Смена владельца readfile.c

```
[root@ibgoloshchapowa guest]# su guest
[guest@ibgoloshchapowa ~]$ cat /home/guest/readfile
cat: /home/guest/readfile: Отказано в доступе
[guest@ibgoloshchapowa ~]$
```

Рис. 9: Чтение readfile.c от имени guest

9. Сменила у программы readfile владельца и установила SetU'D-бит. Проверила, может ли программа readfile прочитать файл readfile.c и файл /etc/shadow
- От имени пользователя guest:

```
[guest@ibgoloshchapowa ~]$ ./readfile readfile.c
bash: ./readfile: Отказано в доступе
[guest@ibgoloshchapowa ~]$ ./readfile /etc/shadow
bash: ./readfile: Отказано в доступе
```

Рис. 10: От имени пользователя guest: readfile.c

- С правами администратора:

```
003117)readfile: 0x00000000 doctype
[guest@ibgoloshchapowa ~]$ su root
Пароль:
[root@ibgoloshchapowa guest]# ./readfile readfile.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

#include <fcntl.h>
#include <sys/stat.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;
}
```

Рис. 11: readfile.c с правами администратора

Чтение файла /etc/shadow

```
[root@ibgoloshchapowa guest]# ./readfile /etc/shadow
root:$6$Q2ZI88n0NO1CREOY$QKPLV15IqLFPU/RJIVaBhZeQeBLu687l6e7V39EDzGhKXRxE093YgKYLUVwt4
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:!!:19607:::::::
dbus:!!:19607:::::::
polkitd:!!:19607:::::::
avahi:!!:19607:::::::
rtkit:!!:19607:::::::
sssd:!!:19607:::::::
pipewire:!!:19607:::::::
libstoragemgmt:!:19607:::::::
systemd-oom:!:19607:::::::
tss:!!:19607:::::::
```

Рис. 12: /etc/shadow

1. Выяснила, что установлен атрибут Sticky на директории /tmp

```
[guest@ibgoloshchapowa ~]$ ls -l / | grep tmp  
drwxrwxrwt. 14 root root 4096 окт  5 22:25 tmp  
[guest@ibgoloshchapowa ~]$
```

Рис. 13: Наличие атрибута Sticky

2. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные»

```
[guest@ibgoloshchapowa ~]$ echo "test" > /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт  5 22:31 /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ chmod o+rw /tmp/file01.txt
[guest@ibgoloshchapowa ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт  5 22:31 /tmp/file01.txt
[guest@ibgoloshchapowa ~]$
```

Рис. 14: file01.txt

3. От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt, дозаписать в файл слово test2, проверить содержимое файла, записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию командой и снова проверить содержимое файла. Затем попробовала удалить файл - не получилось

```
[guest@ibgoloshchapowa ~]$ su guest2
Пароль:
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test
[guest2@ibgoloshchapowa guest]$ echo "test2" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test2
[guest2@ibgoloshchapowa guest]$ echo "test3" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test3
[guest2@ibgoloshchapowa guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@ibgoloshchapowa guest]$
```

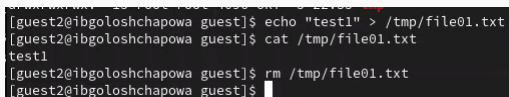
Рис. 15: Операции с file01.txt

4. Повысила свои права до суперпользователя и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории. От пользователя guest2 проверила, что атрибута t у директории /tmp нет

```
[guest2@ibgoloshchapowa guest]$ su -  
Пароль:  
[root@ibgoloshchapowa ~]# chmod -t /tmp  
[root@ibgoloshchapowa ~]# exit  
выход  
[guest2@ibgoloshchapowa guest]$ su guest2  
Пароль:  
[guest2@ibgoloshchapowa guest]$ ls -l / | grep tmp  
drwxrwxrwx. 15 root root 4096 окт  5 22:35 tmp  
[guest2@ibgoloshchapowa guest]$
```

Рис. 16: Снятие атрибута t

5. Повторила предыдущие шаги

A terminal window with a dark background and light-colored text. It shows a series of commands and their outputs. The prompt is [guest2@ibgoloshchapowa guest]\$. The commands are: echo "test1" > /tmp/file01.txt, cat /tmp/file01.txt, and rm /tmp/file01.txt. The outputs are test1 and a blank line.

```
[guest2@ibgoloshchapowa guest]$ echo "test1" > /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$ cat /tmp/file01.txt
test1
[guest2@ibgoloshchapowa guest]$ rm /tmp/file01.txt
[guest2@ibgoloshchapowa guest]$
```

Рис. 17: Повторение операций над файлом

- Повысила свои права до суперпользователя и вернула атрибут `t` на директорию `/tmp`

```
[guest2@ibgoloshchapowa guest]$ su -  
Пароль:  
[root@ibgoloshchapowa ~]# chmod +t /tmp  
[root@ibgoloshchapowa ~]# exit  
выход  
[guest2@ibgoloshchapowa guest]$
```

Рис. 18: Добавление атрибута `t`

В ходе лабораторной работы мне удалось:

- Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
- Получить практических навыков работы в консоли с дополнительными атрибутами.
- Рассмотреть работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.