

Лабораторная работа №5

Кондрашина Мария Сергеевна¹

05.10.2022, Moscow

¹RUDN University, Moscow, Russian Federation

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

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.

Теоретические сведения

Setuid, Setgid и Sticky Bit - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги.

Setuid – это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволяет нам поднять привилегии пользователя в случае, если это необходимо.

Принцип работы Setgid похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

В случае, если Sticky Bit установлен для папки, то файлы в этой папке могут быть удалены только их владельцем, тоже самое верно и для файлов.

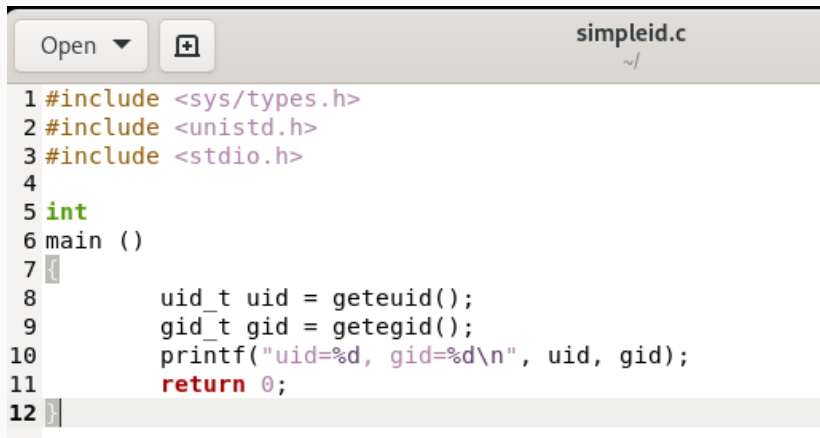
Выполнение лабораторной работы

Создание программы

Подготовка лабораторного стенда

```
[guest@mskondrashina ~]$ su root
Password:
[root@mskondrashina guest]# yum install gcc
Rocky Linux 9 - BaseOS                6.1 kB/s | 3.6 kB      00:00
Rocky Linux 9 - BaseOS                1.4 MB/s | 1.7 MB      00:01
Rocky Linux 9 - AppStream              5.8 kB/s | 3.6 kB      00:00
Rocky Linux 9 - AppStream              2.9 MB/s | 6.0 MB      00:02
Rocky Linux 9 - Extras                 2.9 kB/s | 2.9 kB      00:01
Package gcc-11.2.1-9.4.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@mskondrashina guest]# setenforce 0
[root@mskondrashina guest]# getenforce
Permissive
```

Вошла в систему от имени пользователя guest, создала программу simpleid.c




```
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 }
```

Скомпилировала программу и выполнила ее, также выполнила системную программу `id` и сравнила вывод двух программ - вывелись одинаковые значения

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

Программа simpleid2.c (вывод действительных идентификаторов)

```
Open ▾  simpleid2.c  
~/  
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     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     return 0;  
17 }
```

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

От имени суперпользователя выполнила команды: `chown root:guest /home/guest/simpleid2`, `chmod u+s /home/guest/simpleid2`

```
[guest@mskondrashina ~]$ su root
Password:
[root@mskondrashina guest]# chown root:guest /home/guest/simpleid2
[root@mskondrashina guest]# chmod u+s /home/guest/simpleid2
[root@mskondrashina guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  4 14:40 simpleid2
[root@mskondrashina guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@mskondrashina guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```



```
[root@mskondrashina guest]# chmod g+s /home/guest/simpleid2
[root@mskondrashina guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 26008 Oct  4 14:40 simpleid2
[root@mskondrashina guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@mskondrashina guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Создание файла readfile.c

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

Смена прав так, чтобы только суперпользователь мог прочесть файл

```
[root@mskondrashina guest]# chown root /home/guest/readfile.c  
[root@mskondrashina guest]# chmod 700 /home/guest/readfile.c  
[root@mskondrashina guest]# su - guest
```

```
[root@mskondrashina guest]# su guest  
[guest@mskondrashina ~]$ cat readfile.c  
cat: readfile.c: Permission denied
```

Сменила у программы readfile владельца и установила SetUID-бит

```
[guest@mskondrashina ~]$ su root
Password:
[root@mskondrashina guest]# chown root:guest /home/guest/readfile.c
[root@mskondrashina guest]# chmod u+s /home/guest/readfile.c
[root@mskondrashina guest]# cat /home/guest/readfile.c
```

Проверка чтения файла readfile.c

```
[root@mskondrashina guest]# gcc readfile.c -o readfile
[root@mskondrashina 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;
}
```

[Проверка чтения файла /etc/shadow

```
[root@mskondrashina guest]# ./readfile /etc/shadow
root:$6$Bj0nQ6S/.VKfTpwT$Yg5ZUZMLxL8k.pcct9CngiuWlaZEsrXwysFjZNTa8v0TNg0dsbwno3laZXTXey9XtcXo6b.1WAn/wZob
uYjjP.:0:99999:7:::
bin:!:19123:0:99999:7:::
daemon:!:19123:0:99999:7:::
adm:!:19123:0:99999:7:::
lp:!:19123:0:99999:7:::
sync:!:19123:0:99999:7:::
shutdown:!:19123:0:99999:7:::
halt:!:19123:0:99999:7:::
mail:!:19123:0:99999:7:::
operator:!:19123:0:99999:7:::
games:!:19123:0:99999:7:::
ftp:!:19123:0:99999:7:::
nobody:!:19123:0:99999:7:::
systemd-coredump:!!:19241:::
dbus:!!:19241:::
polkitd:!!:19241:::
rtkit:!!:19241:::
sssd:!!:19241:::
avahi:!!:19241:::
pipewire:!!:19241:::
libstoragemgmt:!!:19241:::
tss:!!:19241:::
geoclue:!!:19241:::
cockpit-ws:!!:19241:::
cockpit-wsinstance:!!:19241:::
setroubleshoot:!!:19241:::
flatpak:!!:19241:::
colord:!!:19241:::
```

Исследование Sticky-бита

Атрибут Sticky на директории /tmp и файл file01.txt

```
[root@mskondrashina guest]# ls -l / | grep tmp
drwxrwxrwt. 15 root root 4096 Oct  4 15:07 tmp
[root@mskondrashina guest]# su guest
[guest@mskondrashina ~]$ echo "test" > /tmp/file01.txt
[guest@mskondrashina ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  4 15:12 /tmp/file01.txt
[guest@mskondrashina ~]$ chmod o+rw /tmp/file01.txt
[guest@mskondrashina ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  4 15:12 /tmp/file01.txt
```

```
[guest@mskondrashina ~]$ su guest2
Password:
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test
[guest2@mskondrashina guest]$ echo "test2" >> /tmp/file01.txt
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test
test2
[guest2@mskondrashina guest]$ echo "test3" > /tmp/file01.txt
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test3
[guest2@mskondrashina guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

```
rm: cannot remove '/tmp/11c01.txt': Operation not permitted
[guest2@mskondrashina guest]$ su -
Password:
[root@mskondrashina ~]# chmod -t /tmp
[root@mskondrashina ~]# exit
logout
```

Взаимодействие guest2 с файлом, когда атрибута t (Sticky-бит) снят с директории /tmp

```
[guest2@mskondrashina guest]$ ls -l / | grep tmp
drwxrwxrwx. 15 root root 4096 Oct  4 15:16 tmp
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test3
[guest2@mskondrashina guest]$ echo "test2" >> /tmp/file01.txt
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test3
test2
[guest2@mskondrashina guest]$ echo "test3" > /tmp/file01.txt
[guest2@mskondrashina guest]$ cat /tmp/file01.txt
test3
[guest2@mskondrashina guest]$ rm /tmp/file01.txt
[guest2@mskondrashina guest]$
```

Возвращение атрибута t (Sticky-бит) на директорию /tmp

```
[guest2@mskondrashina guest]$ su -  
Password:  
[root@mskondrashina ~]# chmod +t /tmp  
[root@mskondrashina ~]# exit  
logout  
[guest2@mskondrashina guest]$ ls -l / | grep tmp  
drwxrwxrwt. 17 root root 4096 Oct  4 15:19 tmp  
[guest2@mskondrashina guest]$
```

- Выполнила лабораторную работу №5.
- Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
- Получила практические навыки работы в консоли с дополнительными атрибутами.
- Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.
2. <https://ruvds.com/ru/helpcenter/suid-sgid-sticky-bit-linux/>