

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Латыпова Диана

5 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Латыпова Диана
- студент группы НФИбд-02-21
- Российский университет дружбы народов
- 1032215005@rudn.ru
- <https://github.com/dlatypova>



Вводная часть

- Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов
- Получение практических навыков работы в консоли с дополнительными атрибутами
- Рассмотрение влияния бита Sticky на запись и удаление файлов

Теоретическое введение

- **UID (User ID)** — идентификатор пользователя, который определяет, от имени какого пользователя выполняется программа
- **GID (Group ID)** — идентификатор группы, определяющий группу, к которой принадлежит пользователь

- **SetUID** — специальный бит, который при установке на файл исполняемой программы позволяет запускать её с правами владельца файла
- **SetGID** работает аналогично, но изменяет эффективный GID на GID владельца файла

Sticky-bit — атрибут директории, который запрещает пользователям удалять файлы, если они не являются их владельцами

Выполнение лабораторной работы

Установка компилятора gcc

```
[guest@user ~]$ su
Password:
[root@user guest]# yum install gcc
Extra Packages for Enterprise Linux 9 - x86_64    56 kB/s | 35 kB    00:00
Extra Packages for Enterprise Linux 9 - x86_64    4.9 MB/s | 23 MB    00:04
packages for the GitHub CLI                      18 kB/s | 3.0 kB    00:00
packages for the GitHub CLI                      10 kB/s | 2.7 kB    00:00
Rocky Linux 9 - BaseOS                           13 kB/s | 4.1 kB    00:00
Rocky Linux 9 - BaseOS                           2.1 MB/s | 2.3 MB    00:01
Rocky Linux 9 - AppStream                         12 kB/s | 4.5 kB    00:00
Rocky Linux 9 - AppStream                         6.3 MB/s | 8.0 MB    00:01
Rocky Linux 9 - Extras                           9.3 kB/s | 2.9 kB    00:00
Visual Studio Code                               11 kB/s | 1.5 kB    00:00
Visual Studio Code                               2.6 MB/s | 5.1 MB    00:01
Package gcc-11.4.1-3.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@user guest]# setenforce 0
[root@user guest]# setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
```

Рис. 1: Установка gcc

Создание и компиляция файла

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

Рис. 2: Задание 1.1-5

Команды chown и chmod

```
chown root:guest /home/guest/simpleid2
```

```
chmod u+s /home/guest/simpleid2
```

```
chmod g+s /home/guest/simpleid2
```

```
[guest@user ~]$ su
Password:
[root@user guest]# chown root:guest /home/guest/simpleid2
[root@user guest]# chmod u+s /home/guest/simpleid2
[root@user guest]# ls -l simpleid2
-rwxr-xr-x. 1 root guest 17720 Oct 5 10:30 simpleid2
[root@user guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@user guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r
unconfined_t:s0-s0:c0.c1023
[root@user guest]# chown root:guest /home/guest/simpleid2
[root@user guest]# chmod g+s /home/guest/simpleid2
[root@user guest]# ls -l simpleid2
-rwxr-sr-x. 1 root guest 17720 Oct 5 10:30 simpleid2
[root@user guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@user guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r
unconfined_t:s0-s0:c0.c1023
```

Рис. 3: Задание 1.8-12

```
[guest@user ~]$ touch readfile.c  
[guest@user ~]$ gcc readfile.c -o readfile
```

Рис. 4: Задание 1.13-14

```
[guest@user ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@user ~]$ ./readfile readfile.c
bash: ./readfile: Permission denied
[guest@user ~]$ ./readfile /etc/shadow
bash: ./readfile: Permission denied
```

Рис. 5: Задание 1.16-19 (1)

Проверка изменения прав (2)

```
[root@user guest]# cat 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@user 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@user guest]# ./readfile /etc/shadow
root:$6$5i0rpMKsyRp49od.$6leG0dcDz0MWfLjF10ntCzkP5XB2WH4ntum71kn4582C8FI
oolPeowhWX/7EgcMzzRhd.t5m2ypirvlqEq.q.:0:99999:7:::
bin:~:19820:0:99999:7:::
```

```
chmod o+rw /tmp/file01.txt
```

```
[guest@user ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  5 10:45 tmp
[guest@user ~]$ echo "test" > /tmp/file01.txt
[guest@user ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  5 10:48 /tmp/file01.txt
[guest@user ~]$ chmod o+rw /tmp/file01.txt
[guest@user ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  5 10:48 /tmp/file01.txt
```

Рис. 7: Задание 2.1-4

Исследование sticky-бита (2)

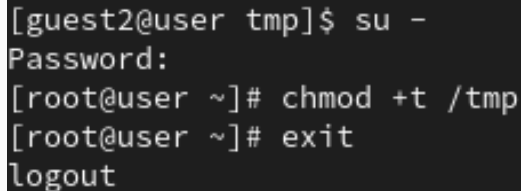
`chmod -t /tmp`

```
[guest@user tmp]$ su guest2
Password:
[guest2@user tmp]$ cat /tmp/file01.txt
test
[guest2@user tmp]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@user tmp]$ cat /tmp/file01.txt
test
[guest2@user tmp]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@user tmp]$ cat /tmp/file01.txt
test
[guest2@user tmp]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@user tmp]$ su -
Password:
[root@user ~]# chmod -t /tmp
[root@user ~]# exit
logout
[guest2@user tmp]$ ls -l | grep tmp
drwxrwxrwx. 18 root root 4096 Oct  5 11:01 tmp
[guest2@user tmp]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@user tmp]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
```

Рис. 8: Задание 2.5-14

Исследование sticky-бита (3)

```
chmod +t /tmp
```



```
[guest2@user tmp]$ su -  
Password:  
[root@user ~]# chmod +t /tmp  
[root@user ~]# exit  
logout
```

Рис. 9: Задание 2.15

Выводы

- Изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов
- Получены практические навыки работы в консоли с дополнительными атрибутами
- Рассмотрено влияние бита Sticky на запись и удаление файлов