

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибуто

Белов М. С.

2 октября 2024

Российский университет дружбы народов, Москва, Россия

Задача

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 лабораторной работы

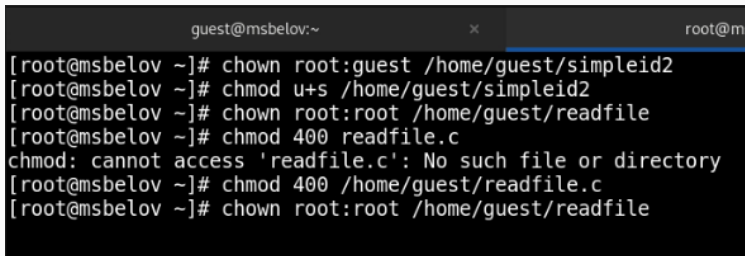
Создание программы

1. От имени пользователя *guest* создадим две программы *simpleid* и *simpleid2*. Также создадим программу *readfile*

```
guest@msbelov:~  
guest@msbelov ~]$ touch simpleid.c  
guest@msbelov ~]$ vim simpleid.c  
guest@msbelov ~]$ gcc simpleid.c -o simpleid  
guest@msbelov ~]$ ls  
simpleid simpleid.c  
guest@msbelov ~]$ ./simpleid  
id=1001, gid=1001  
guest@msbelov ~]$ id  
id=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:  
nconfined t:s0-s0:c0.c1023  
guest@msbelov ~]$ vim simpleid.c  
guest@msbelov ~]$ mv simpleid.c simpleid2.c  
guest@msbelov ~]$ ls  
simpleid simpleid2.c  
guest@msbelov ~]$ gcc simpleid2.c -o simpleid2  
guest@msbelov ~]$ ./simpleid2  
_uid=1001, e_gid=1001  
eal uid=1001, real_gid=1001  
guest@msbelov ~]$ ls -l simpleid  
rwxr-xr-x. 1 guest guest 17616 Oct  2 03:55 simpleid  
guest@msbelov ~]$ ls -l simpleid2  
rwsr-xr-x. 1 root guest 17720 Oct  2 03:58 simpleid2  
guest@msbelov ~]$ ./simpleid2  
_uid=0, e_gid=1001  
eal uid=1001, real_gid=1001
```

Создание программы

От имени суперпользователя выполним некоторые команды и проверим их работу:

A terminal window with a dark background. The title bar shows two tabs: 'guest@msbelov:~' and 'root@ms'. The terminal content shows a series of commands executed as root. The first three commands are successful: 'chown root:guest /home/guest/simpleid2', 'chmod u+s /home/guest/simpleid2', and 'chown root:root /home/guest/readfile'. The next two commands fail: 'chmod 400 readfile.c' results in 'chmod: cannot access 'readfile.c': No such file or directory', and 'chmod 400 /home/guest/readfile.c' is successful. The final command 'chown root:root /home/guest/readfile' is also successful.

```
guest@msbelov:~ x root@ms
[root@msbelov ~]# chown root:guest /home/guest/simpleid2
[root@msbelov ~]# chmod u+s /home/guest/simpleid2
[root@msbelov ~]# chown root:root /home/guest/readfile
[root@msbelov ~]# chmod 400 readfile.c
chmod: cannot access 'readfile.c': No such file or directory
[root@msbelov ~]# chmod 400 /home/guest/readfile.c
[root@msbelov ~]# chown root:root /home/guest/readfile
```

Рис. 2: Команды от имени root

2. Выясним установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test. Просмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные». Также попробуем снять атрибут *t*.

Исследование Sticky-бита

```
guest2@msbelov:/home/guest x root@msbelov:~
[guest@msbelov ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct  2 04:02 tmp
[guest@msbelov ~]$ echo "test" > /tmp/file01.txt
[guest@msbelov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  2 04:03 /tmp/file01.txt
[guest@msbelov ~]$ chmod o+rw /tmp/file01.txt
[guest@msbelov ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  2 04:03 /tmp/file01.txt
[guest@msbelov ~]$ su guest2
Password:
[guest2@msbelov guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@msbelov guest]$ cat /tmp/file01.txt
test
[guest2@msbelov guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@msbelov guest]$ cat /tmp/file01.txt
test
[guest2@msbelov guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@msbelov guest]$ su -
Password:
[root@msbelov ~]# chmod -t /tmp
[root@msbelov ~]# exit
logout
[guest2@msbelov guest]$ ls -l / | grep tmp
drwxrwxrwx. 19 root root 4096 Oct  2 04:06 tmp
[guest2@msbelov guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@msbelov guest]$ rm /tmp/file01.txt
```


Вывод

В ходе работы я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.