

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Джафер Идрисов

25 марта, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

Цель лабораторной 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.

Выполнение лабораторной работы

Программа simpleid

```
-----
guest@didrisov:~$ mkdir lab5
guest@didrisov:~$ cd lab5/
guest@didrisov:~/lab5$ touch simpleid.c
guest@didrisov:~/lab5$
guest@didrisov:~/lab5$ gcc simpleid.c
guest@didrisov:~/lab5$ gcc simpleid.c -o simpleid
guest@didrisov:~/lab5$ ./simpleid
uid=1001, gid=1001
guest@didrisov:~/lab5$ od
^C
guest@didrisov:~/lab5$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
guest@didrisov:~/lab5$ █
```

Рис. 1: результат программы simpleid

Программа simpleid2

```
guest@didrisov:~/lab5$ ./simpleid2
guest@didrisov:~/lab5$ touch simpleid2.c
guest@didrisov:~/lab5$ gcc simpleid2.c
guest@didrisov:~/lab5$ gcc simpleid2.c -o simpleid2
guest@didrisov:~/lab5$ ./simpleid2
uid=1001, gid=1001
guest@didrisov:~/lab5$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
guest@didrisov:~/lab5$ su
Пароль:
root@didrisov:/home/guest/lab5# chown root:guest simpleid2
root@didrisov:/home/guest/lab5# chmod u+s simpleid2
root@didrisov:/home/guest/lab5# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
root@didrisov:/home/guest/lab5# id
uid=0(root) gid=0(root) rpyrny=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c10
23
root@didrisov:/home/guest/lab5# chmod g+s simpleid2
root@didrisov:/home/guest/lab5# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
root@didrisov:/home/guest/lab5#
exit
guest@didrisov:~/lab5$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
guest@didrisov:~/lab5$ █
```

Рис. 2: результат программы simpleid2

Программа readfile

```
guest@didrisov:~/lab5$ touch readfile.c
guest@didrisov:~/lab5$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
    20 | while (bytes_read == (buffer));
        |                      ^~
guest@didrisov:~/lab5$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
    20 | while (bytes_read == (buffer));
        |                      ^~
guest@didrisov:~/lab5$ su
Пароль:
root@didrisov:/home/guest/lab5# chown root:root readfile
root@didrisov:/home/guest/lab5# chmod -rwx readfile.c
root@didrisov:/home/guest/lab5# chmod u+s readfile
root@didrisov:/home/guest/lab5# exit
guest@didrisov:~/lab5$ cat readfile.c
cat: readfile.c: Отказано в доступе
guest@didrisov:~/lab5$ ./readfile readfile.c
#include <stdio.h>
guest@didrisov:~/lab5$ ./readfile /etc/shadow
root:$y$9T$zLZFguest@didrisov:~/lab5$
guest@didrisov:~/lab5$ █
```

Рис. 3: результат программы readfile

Исследование Sticky-бита

```
guest@didrisov:~/lab5$  
guest@didrisov:~/lab5$ cd /tmp  
guest@didrisov:/tmp$ echo test >> file01.txt  
guest@didrisov:/tmp$ chmod g+rx file01.txt  
guest@didrisov:/tmp$ su guest2  
Пароль:  
guest2@didrisov:/tmp$ cd /tmp  
guest2@didrisov:/tmp$ cat file01.txt  
test  
guest2@didrisov:/tmp$ echo test2 >> file01.txt  
guest2@didrisov:/tmp$ cat file01.txt  
test  
test2  
guest2@didrisov:/tmp$ echo test3 >> file01.txt  
guest2@didrisov:/tmp$ echo test3 > file01.txt  
guest2@didrisov:/tmp$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
guest2@didrisov:/tmp$ su  
Пароль:  
root@didrisov:/tmp# chmod -t /tmp/  
root@didrisov:/tmp#  
exit  
guest2@didrisov:/tmp$ █
```

Рис. 4: исследование Sticky-бита

Выводы

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.