

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Тихонова Екатерина

2 октября, 2023, 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

```
exit
[guest@eatihonova ~]$ mkdir lab5
[guest@eatihonova ~]$ cd lab5
[guest@eatihonova lab5]$ touch simpleid.c
[guest@eatihonova lab5]$ mv simpleid.c simpleid.c
[guest@eatihonova lab5]$ gcc simpleid.c
[guest@eatihonova lab5]$ gcc simpleid.c -o simpleid
[guest@eatihonova lab5]$ ./simpleid
uid=1001, gid=1001
[guest@eatihonova lab5]$ od
^C
[guest@eatihonova lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel)
_t:s0-s0:c0.c1023
[guest@eatihonova lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@eatihonova lab5]$ touch simpleid2.c
[guest@eatihonova lab5]$ gcc simpleid2.c
[guest@eatihonova lab5]$ gcc simpleid2.c -o simpleid2
[guest@eatihonova lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@eatihonova lab5]$ su
Пароль:
[root@eatihonova lab5]# chown root:guest simpleid2
[root@eatihonova lab5]# chown u+s simpleid2
chown: неверный пользователь: «u+s»
[root@eatihonova lab5]# chmod u+s simpleid2
[root@eatihonova lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@eatihonova lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:u
[root@eatihonova lab5]# chmod g+s simpleid2
[root@eatihonova lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@eatihonova lab5]#
6 exit
[guest@eatihonova lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@eatihonova lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@eatihonova lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@eatihonova lab5]$ ls -l
итого 124
-rwxr-xr-x. 1 guest guest 26008 окт  2 18:26 a.out
-rwsr-xr-x. 1 root  root 26008 окт  2 18:26 readfile
----- 1 guest guest  386 окт  2 18:26 readfile.c
-rwxr-xr-x. 1 guest guest 25960 окт  2 18:22 simpleid
-rwsr-sr-x. 1 root  guest 26064 окт  2 18:24 simpleid2
-rw-r--r--. 1 guest guest  295 окт  2 18:23 simpleid2.c
-rw-r--r--. 1 guest guest  171 окт  2 18:21 simpleid.c
[guest@eatihonova lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@eatihonova lab5]$
[guest@eatihonova lab5]$ ./readfile /etc/shadow
root:$6$0mJpklj[guest@eatihonova lab5]$
[guest@eatihonova lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@eatihonova lab5]$  
[guest@eatihonova lab5]$ cd /tmp  
[guest@eatihonova tmp]$ echo test >> file01.txt  
[guest@eatihonova tmp]$ chmod 777 file01.txt  
[guest@eatihonova tmp]$ su guest2  
Пароль:  
[guest2@eatihonova tmp]$ echo test >> file01.txt  
[guest2@eatihonova tmp]$ echo test > file01.txt  
[guest2@eatihonova tmp]$ cat file01.txt  
test  
[guest2@eatihonova tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@eatihonova tmp]$ su  
Пароль:  
[root@eatihonova tmp]# chmod -t /tmp  
[root@eatihonova tmp]#  
exit  
[guest2@eatihonova tmp]$ rm file01.txt  
[guest2@eatihonova tmp]$  
[guest2@eatihonova tmp]$
```

Figure 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.