

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Владислав Ракинцев

22 сентября, 2024, 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@vprakincev ~]$  
[guest@vprakincev ~]$  
[guest@vprakincev ~]$ cd  
[guest@vprakincev ~]$ mkdir lab5  
[guest@vprakincev ~]$ cd lab5/  
[guest@vprakincev lab5]$ touch simoleid.c  
[guest@vprakincev lab5]$ mv simoleid.c simpleid.c  
[guest@vprakincev lab5]$ gedit simpleid.c  
[guest@vprakincev lab5]$ gcc simpleid.c  
[guest@vprakincev lab5]$ gcc simpleid.c -o simpleid  
[guest@vprakincev lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@vprakincev lab5]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@vprakincev lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@vprakincev lab5]$  
[guest@vprakincev lab5]$ gcc simpleid2.c  
[guest@vprakincev lab5]$ gcc simpleid2.c -o simpleid2  
[guest@vprakincev lab5]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@vprakincev lab5]$ su  
Пароль:  
[root@vprakincev lab5]# chown root:guest simpleid2  
[root@vprakincev lab5]# chmod u+s simpleid2  
[root@vprakincev lab5]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@vprakincev lab5]# id  
uid=0(root) gid=0(root) rpynmw=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@vprakincev lab5]# chmod g+s simpleid2  
[root@vprakincev lab5]# ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=0  
[root@vprakincev lab5]#  
exit  
[guest@vprakincev lab5]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@vprakincev lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@vprakincev lab5]$ touch readfile.c
[guest@vprakincev lab5]$ gedit readfile.c
[guest@vprakincev lab5]$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
   20 | while (bytes_read == (buffer));
      |                      ^~
[guest@vprakincev 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@vprakincev lab5]$ su
Пароль:
[root@vprakincev lab5]# chown root:root readfile
[root@vprakincev lab5]# chmod -rwx readfile.c
[root@vprakincev lab5]# chmod u+s readfile
[root@vprakincev lab5]#
exit
[guest@vprakincev lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@vprakincev lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@vprakincev lab5]$
[guest@vprakincev lab5]$ ./readfile /etc/shadow
root:$6$0mJpKglj[guest@vprakincev lab5]$
[guest@vprakincev lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

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