

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Александр Атанесов

13 марта, 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

```
[root@alexatanesov guest]# setenforce 0
[root@alexatanesov guest]#
exit
[guest@alexatanesov ~]$ getenforce
Permissive
[guest@alexatanesov ~]$ cd
[guest@alexatanesov ~]$ mkdir lab5
[guest@alexatanesov ~]$ cd lab5/
[guest@alexatanesov lab5]$ touch simpleid.c
[guest@alexatanesov lab5]$ gedit simpleid.c
[guest@alexatanesov lab5]$ gcc simpleid.c
[guest@alexatanesov lab5]$ gcc simpleid.c -o simpleid
[guest@alexatanesov lab5]$ ./simpleid
uid=1001, gid=1001
[guest@alexatanesov lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfine
d_t:s0-s0:c0.c1023
[guest@alexatanesov lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

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

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@alexatanesov lab5]$  
[guest@alexatanesov lab5]$ gcc readfile.c  
readfile.c: В функции «main»:  
readfile.c:20:19: предупреждение: сравнение указателя и целого  
20 | while (bytes_read == (buffer));  
    |                   ^~  
[guest@alexatanesov 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@alexatanesov lab5]$ su  
Пароль:  
[root@alexatanesov lab5]# chown root:root readfile  
[root@alexatanesov lab5]# chmod -rwx readfile.c  
[root@alexatanesov lab5]# chmod u+s readfile  
[root@alexatanesov lab5]#  
exit  
[guest@alexatanesov lab5]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@alexatanesov lab5]$ ./readfile readfile.c  
#include <stdio.h>[guest@alexatanesov lab5]$  
[guest@alexatanesov lab5]$ ./readfile /etc/shadow  
root:$6$0mJpkg1j[guest@alexatanesov lab5]$  
[guest@alexatanesov lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@alexatanesov lab5]$  
[guest@alexatanesov lab5]$ cd /tmp  
[guest@alexatanesov tmp]$ echo test >> file01.txt  
[guest@alexatanesov tmp]$ chmod g+rxw file01.txt  
[guest@alexatanesov tmp]$ su guest2  
Пароль:  
[guest2@alexatanesov tmp]$ cat file01.txt  
test  
[guest2@alexatanesov tmp]$ echo test2 >> file01.txt  
[guest2@alexatanesov tmp]$ cat file01.txt  
test  
test2  
[guest2@alexatanesov tmp]$ echo test3 > file01.txt  
[guest2@alexatanesov tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@alexatanesov tmp]$ su  
Пароль:  
[root@alexatanesov tmp]# chmod -t /tmp  
chmod: невозможно получить доступ к '/tmp': Нет такого файла или каталога  
[root@alexatanesov tmp]#  
exit  
[guest2@alexatanesov tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@alexatanesov tmp]$ su  
Пароль:  
[root@alexatanesov tmp]# chmod -t /tmp  
[root@alexatanesov tmp]#  
exit  
[guest2@alexatanesov tmp]$ rm file01.txt  
[guest2@alexatanesov 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.