

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Александр Фирсов

28 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

```
Permissive
[guest@afirsov ~]$ cd
[guest@afirsov ~]$ mkdir lab5
[guest@afirsov ~]$ cd lab5/
[guest@afirsov lab5]$ touch simpleid.c
[guest@afirsov lab5]$ gedit simpleid.c
[guest@afirsov lab5]$ gcc simpleid.c
[guest@afirsov lab5]$ gcc simpleid.c -o simpleid
[guest@afirsov lab5]$ ./simpleid
uid=1001, gid=1001
[guest@afirsov lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(v
.c1023
[guest@afirsov lab5]$
```

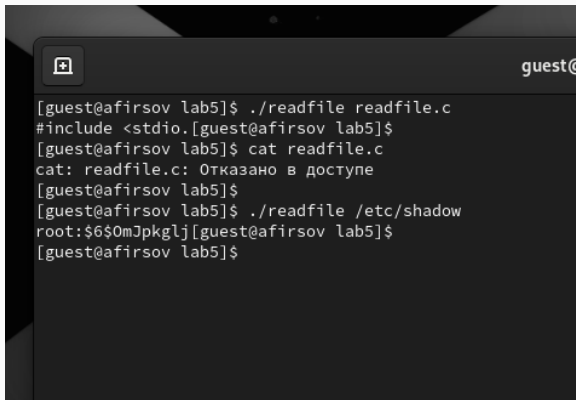
Figure 1: результат программы simpleid

Программа simpleid2

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

Figure 2: результат программы simpleid2

Программа readfile

A terminal window with a dark background and light text. The window title bar shows a plus icon on the left and 'guest@' on the right. The terminal content shows a series of commands and their outputs. The first command is './readfile readfile.c', which outputs '#include <stdio.'. The second command is 'cat readfile.c', which outputs an error message in Russian: 'cat: readfile.c: Отказано в доступе'. The third command is './readfile /etc/shadow', which outputs a root shell prompt '\$6\$0mJpkglj'.

```
[guest@afirsov lab5]$ ./readfile readfile.c
#include <stdio.[guest@afirsov lab5]$
[guest@afirsov lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@afirsov lab5]$
[guest@afirsov lab5]$ ./readfile /etc/shadow
root:$6$0mJpkglj[guest@afirsov lab5]$
[guest@afirsov lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@afirsov lab5]$  
[guest@afirsov lab5]$ cd /tmp  
[guest@afirsov tmp]$ echo test >> file01.txt  
[guest@afirsov tmp]$ chmod g+rw file01.txt  
[guest@afirsov tmp]$ su guest2  
Пароль:  
[guest2@afirsov tmp]$ cat file01.txt  
test  
[guest2@afirsov tmp]$ echo test >> file01.txt  
[guest2@afirsov tmp]$ echo 123 > file01.txt  
[guest2@afirsov tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@afirsov tmp]$ su  
Пароль:  
[root@afirsov tmp]# chmod -t /tmp  
[root@afirsov tmp]#  
exit  
[guest2@afirsov tmp]$ rm file01.txt  
[guest2@afirsov 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.