

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Танаков Артем НБИ-01-20

29 сентября, 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

```
[guest@aatanakov ~]$  
[guest@aatanakov ~]$ cd  
[guest@aatanakov ~]$ mkdir lab5  
[guest@aatanakov ~]$ cd lab5/  
[guest@aatanakov lab5]$ touch simpleid.c  
[guest@aatanakov lab5]$ gcc simpleid.c  
[guest@aatanakov lab5]$ gcc simpleid.c -o simpleid  
[guest@aatanakov lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@aatanakov lab5]$ id  
uid=1001(guest) gid=1001(guest) rpyннw=1001(guest),10(wheel) контекст=unconfined  
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@aatanakov lab5]$
```

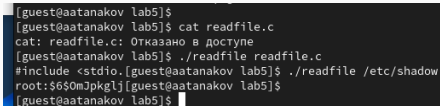
Figure 1: результат программы simpleid

Программа simpleid2

```
real_uid=1001, real_gid=1001
[guest@aatanakov lab5]$ su
Пароль:
[root@aatanakov lab5]# chown root:guest simpleid2
[root@aatanakov lab5]# chmod u+s simpleid2
[root@aatanakov lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@aatanakov lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@aatanakov lab5]# chmod g+s simpleid2
[root@aatanakov lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@aatanakov lab5]#
exit
[guest@aatanakov lab5]$
[guest@aatanakov lab5]$ touch readfile.c
[guest@aatanakov lab5]$
[guest@aatanakov lab5]$ gcc readfile.c
readfile.c: В функции «main»:
```

Figure 2: результат программы simpleid2

Программа readfile

A terminal window with a dark background and light-colored text. The text shows a sequence of commands and their outputs in a shell environment. The prompt is [guest@aatanakov lab5]\$. The first command is cat readfile.c, which results in an error message: cat: readfile.c: Отказано в доступе. The second command is ./readfile readfile.c, which results in a segmentation fault: #include <stdio.h>[guest@aatanakov lab5]\$. The third command is ./readfile /etc/shadow, which results in a root shell: root:\$6\$0mJpkglj[guest@aatanakov lab5]\$. The prompt returns to [guest@aatanakov lab5]\$.

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

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@aaatanakov labs]$ cd /tmp
[guest@aaatanakov tmp]$ echo test >> /tmp/file01.txt
[guest@aaatanakov tmp]$ chmod g+rx file01.txt
[guest@aaatanakov tmp]$ chmod o+rx file01.txt
[guest@aaatanakov tmp]$ su guest2
Пароль:
[guest2@aaatanakov tmp]$ cd /tmp
[guest2@aaatanakov tmp]$ cat file01.txt
test
[guest2@aaatanakov tmp]$ echo test >> file01.txt
[guest2@aaatanakov tmp]$ echo test > file01.txt
[guest2@aaatanakov tmp]$ rm file01.txt
rm: невозможно удалить 'file01.txt': Операция не позволена
[guest2@aaatanakov tmp]$ su
Пароль:
[root@aaatanakov tmp]# chmod -t file01.txt
[root@aaatanakov tmp]#
exit
[guest2@aaatanakov tmp]$ echo test >> file01.txt
[guest2@aaatanakov tmp]$ echo test > file01.txt
[guest2@aaatanakov tmp]$ rm file01.txt
rm: невозможно удалить 'file01.txt': Операция не позволена
[guest2@aaatanakov tmp]$ su
Пароль:
[root@aaatanakov tmp]# shmod -t /tmp
bash: shmod: command not found...
Similar command is: 'chmod'
[root@aaatanakov tmp]# chmod -t /tmp
[root@aaatanakov tmp]#
exit
[guest2@aaatanakov tmp]$ rm file01.txt
[guest2@aaatanakov 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.