

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Князьков Геннадий НБИ-01-19

3 октября, 2022, 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.

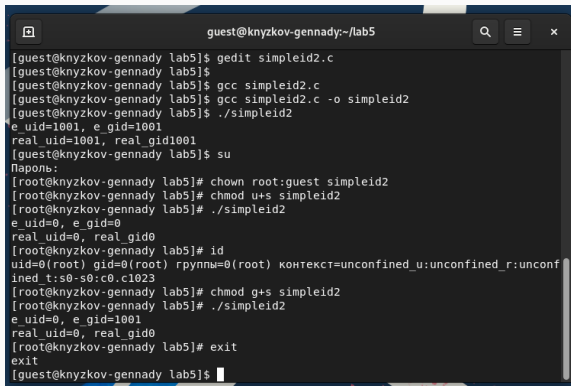
Выполнение лабораторной работы

Программа simpleid

```
[guest@knyzkov-gennady ~]$ cd
[guest@knyzkov-gennady ~]$ mkdir lab5
[guest@knyzkov-gennady ~]$ cd lab5/
[guest@knyzkov-gennady lab5]$ touch simpleid.c
[guest@knyzkov-gennady lab5]$ touch simpleid2.c
[guest@knyzkov-gennady lab5]$ touch readfile.c
[guest@knyzkov-gennady lab5]$ gedit simpleid.c
[guest@knyzkov-gennady lab5]$ gcc simpleid.c
[guest@knyzkov-gennady lab5]$ gcc simpleid.c -o simpleid
[guest@knyzkov-gennady lab5]$ ./simpleid
uid=1001, gid=1001
[guest@knyzkov-gennady lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@knyzkov-gennady lab5]$
```

Figure 1: результат программы simpleid

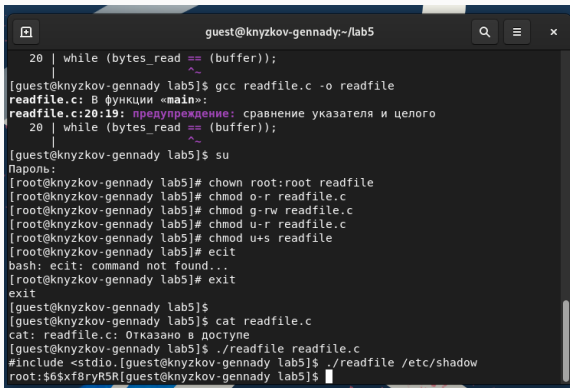
Программа simpleid2



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

Figure 2: результат программы simpleid2

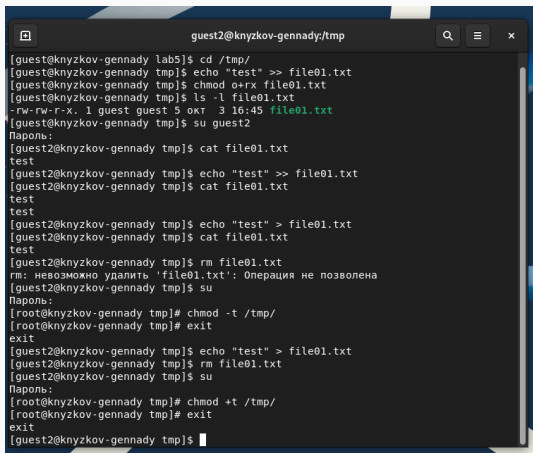
Программа readfile



```
20 | while (bytes_read == (buffer));  
    ^~  
[guest@knyzkov-gennady 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@knyzkov-gennady lab5]$ su  
Пароль:  
[root@knyzkov-gennady lab5]# chown root:root readfile  
[root@knyzkov-gennady lab5]# chmod o-r readfile.c  
[root@knyzkov-gennady lab5]# chmod g-rw readfile.c  
[root@knyzkov-gennady lab5]# chmod u-r readfile.c  
[root@knyzkov-gennady lab5]# chmod u+s readfile  
[root@knyzkov-gennady lab5]# ecit  
bash: ecit: command not found...  
[root@knyzkov-gennady lab5]# exit  
exit  
[guest@knyzkov-gennady lab5]$  
[guest@knyzkov-gennady lab5]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@knyzkov-gennady lab5]$ ./readfile readfile.c  
#include <stdio.h>  
[guest@knyzkov-gennady lab5]$ ./readfile /etc/shadow  
root:$6$xf87rY5R[guest@knyzkov-gennady lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
guest2@knyzkov-gennady:/tmp
[guest@knyzkov-gennady lab5]$ cd /tmp/
[guest@knyzkov-gennady tmp]$ echo "test" >> file01.txt
[guest@knyzkov-gennady tmp]$ chmod o+rx file01.txt
[guest@knyzkov-gennady tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 guest guest 5 окт  3 16:45 file01.txt
[guest@knyzkov-gennady tmp]$ su guest2
Пароль:
[guest2@knyzkov-gennady tmp]$ cat file01.txt
test
[guest2@knyzkov-gennady tmp]$ echo "test" >> file01.txt
[guest2@knyzkov-gennady tmp]$ cat file01.txt
test
test
[guest2@knyzkov-gennady tmp]$ echo "test" > file01.txt
[guest2@knyzkov-gennady tmp]$ cat file01.txt
test
[guest2@knyzkov-gennady tmp]$ rm file01.txt
rm: невозможно удалить 'file01.txt': Операция не позволена
[guest2@knyzkov-gennady tmp]$ su
Пароль:
[root@knyzkov-gennady tmp]# chmod -t /tmp/
[root@knyzkov-gennady tmp]# exit
exit
[guest2@knyzkov-gennady tmp]$ echo "test" > file01.txt
[guest2@knyzkov-gennady tmp]$ rm file01.txt
[guest2@knyzkov-gennady tmp]$ su
Пароль:
[root@knyzkov-gennady tmp]# chmod +t /tmp/
[root@knyzkov-gennady tmp]# exit
exit
[guest2@knyzkov-gennady 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.