

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Романов Дмитрий Романович НБИ-01-19

4 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.

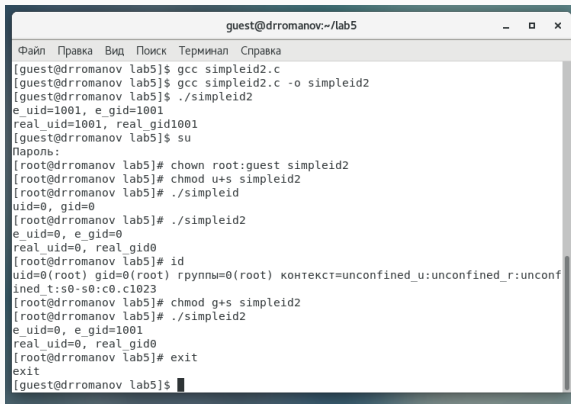
Выполнение лабораторной работы

Программа simpleid

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

Figure 1: результат программы simpleid

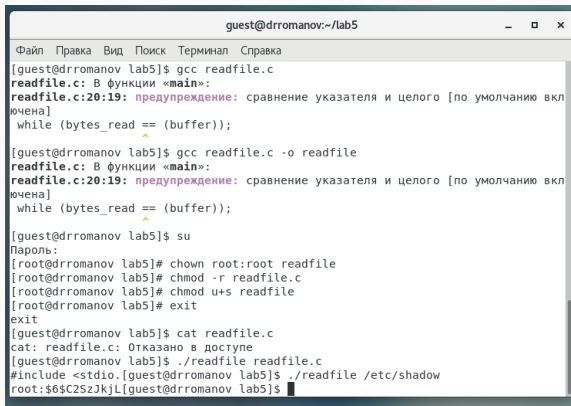
Программа simpleid2



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

Figure 2: результат программы simpleid2

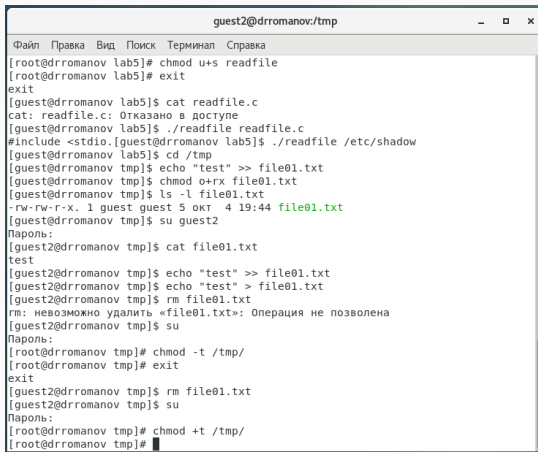
Программа readfile



```
guest@drromanov:~/lab5
Файл Правка Вид Поиск Терминал Справка
[guest@drromanov lab5]$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
    while (bytes_read == (buffer));
                      ^
[guest@drromanov lab5]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
    while (bytes_read == (buffer));
                      ^
[guest@drromanov lab5]$ su
Пароль:
[root@drromanov lab5]# chown root:root readfile
[root@drromanov lab5]# chmod -r readfile.c
[root@drromanov lab5]# chmod u+s readfile
[root@drromanov lab5]# exit
exit
[guest@drromanov lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@drromanov lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@drromanov lab5]$ ./readfile /etc/shadow
root:$6$C2SzJkL[guest@drromanov lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
guest2@drromanov:tmp
Файл Правка Вид Поиск Терминал Справка
[root@drromanov lab5]# chmod u+s readfile
[root@drromanov lab5]# exit
exit
[guest@drromanov lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@drromanov lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@drromanov lab5]$ ./readfile /etc/shadow
[guest@drromanov lab5]$ cd /tmp
[guest@drromanov tmp]$ echo "test" >> file01.txt
[guest@drromanov tmp]$ chmod o+rx file01.txt
[guest@drromanov tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 guest guest 5 окт  4 19:44 file01.txt
[guest@drromanov tmp]$ su guest2
Пароль:
[guest2@drromanov tmp]$ cat file01.txt
test
[guest2@drromanov tmp]$ echo "test" >> file01.txt
[guest2@drromanov tmp]$ echo "test" > file01.txt
[guest2@drromanov tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@drromanov tmp]$ su
Пароль:
[root@drromanov tmp]# chmod -t /tmp/
[root@drromanov tmp]# exit
exit
[guest2@drromanov tmp]$ rm file01.txt
[guest2@drromanov tmp]$ su
Пароль:
[root@drromanov tmp]# chmod +t /tmp/
[root@drromanov 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.