

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Егина Ангелина

22 сентября, 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

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

Figure 1: результат программы simpleid

# Программа simpleid2

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

Figure 2: результат программы simpleid2

# Программа readfile

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

Figure 3: результат программы readfile



# Исследование Sticky-бита

```
[guest@aegina ~]$  
[guest@aegina ~]$ echo test >> /tmp/file01.txt  
[guest@aegina ~]$ su g+rxw /tmp/file01.txt  
su: user g+rxw does not exist or the user entry does not contain all the required fields  
[guest@aegina ~]$ chmod g+rxw /tmp/file01.txt  
[guest@aegina ~]$ su guest2  
Пароль:  
[guest2@aegina guest]$ cd /tmp  
[guest2@aegina tmp]$ cat file01.txt  
test  
[guest2@aegina tmp]$ echo test2 >> file01.txt  
[guest2@aegina tmp]$ cat file01.txt  
test  
test2  
[guest2@aegina tmp]$ echo test3 > file01.txt  
[guest2@aegina tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@aegina tmp]$ su  
Пароль:  
[root@aegina tmp]# chmod -t /tmp  
[root@aegina tmp]#  
exit  
[guest2@aegina tmp]$ echo test2 >> file01.txt  
[guest2@aegina tmp]$ rm file01.txt  
[guest2@aegina 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.