

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Alexey A. Shemyakin¹

13 November, 2021 Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

Цели и задачи

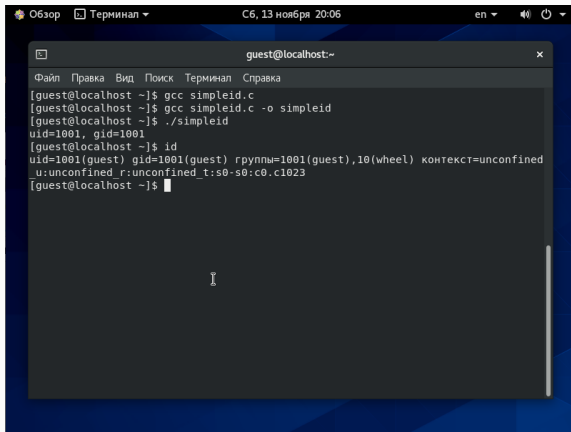
- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться 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

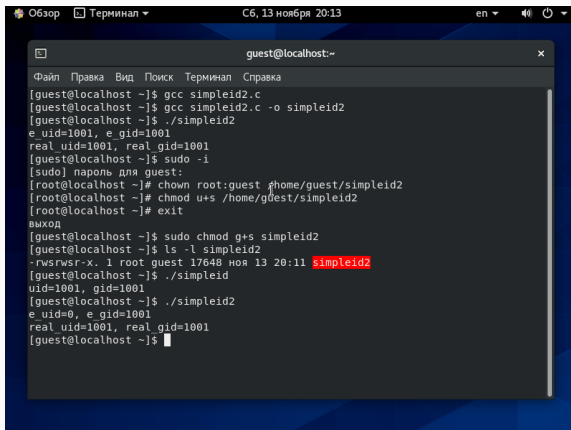


The screenshot shows a terminal window titled "guest@localhost:~" with a menu bar containing "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal output shows the following commands and results:

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

Figure 1: результат программы simpleid

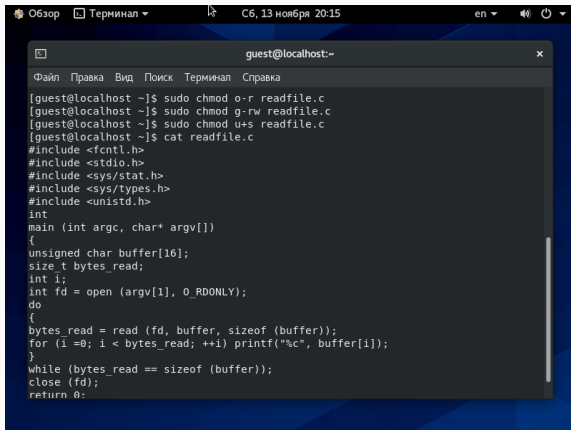
Программа simpleid2



```
Обзор Терминал C6, 13 ноября 20:13 en 0 0
guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
[guest@localhost ~]$ gcc simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$ sudo -i
[sudo] пароль для guest:
[root@localhost ~]# chown root:guest /home/guest/simpleid2
[root@localhost ~]# chmod u+s /home/guest/simpleid2
[root@localhost ~]# exit
выход
[guest@localhost ~]$ sudo chmod g+s simpleid2
[guest@localhost ~]$ ls -l simpleid2
-rwsrwsr-x. 1 root guest 17648 ноя 13 20:11 simpleid2
[guest@localhost ~]$ ./simpleid2
uid=1001, gid=1001
[guest@localhost ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$
```

Figure 2: результат программы simpleid2

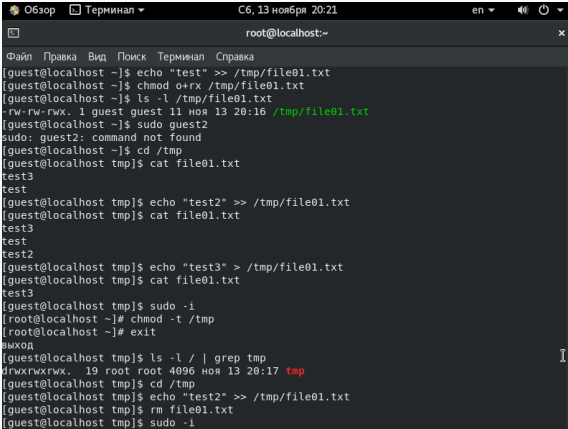
Программа readfile



```
guest@localhost:~  
[guest@localhost ~]$ sudo chmod o-r readfile.c  
[guest@localhost ~]$ sudo chmod g-rw readfile.c  
[guest@localhost ~]$ sudo chmod u+s readfile.c  
[guest@localhost ~]$ cat readfile.c  
#include <fcntl.h>  
#include <stdio.h>  
#include <sys/stat.h>  
#include <sys/types.h>  
#include <unistd.h>  
int  
main (int argc, char* argv[])  
{  
    unsigned char buffer[16];  
    size_t bytes_read;  
    int i;  
    int fd = open (argv[1], O_RDONLY);  
    do  
    {  
        bytes_read = read (fd, buffer, sizeof (buffer));  
        for (i=0; i < bytes_read; ++i) printf("%c", buffer[i]);  
    }  
    while (bytes_read == sizeof (buffer));  
    close (fd);  
    return 0;  
}
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
Обзор Терминал C6, 13 ноября 20:21 en  [иконка] [иконка]
root@localhost:~

Файл Правка Вид Поиск Терминал Справка
[guest@localhost ~]$ echo "test" >> /tmp/file01.txt
[guest@localhost ~]$ chmod o+rx /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-rwx. 1 guest guest 11 ноя 13 20:16 /tmp/file01.txt
[guest@localhost ~]$ sudo guest2
sudo: guest2: command not found
[guest@localhost ~]$ cd /tmp
[guest@localhost tmp]$ cat file01.txt
test3
test
[guest@localhost tmp]$ echo "test2" >> /tmp/file01.txt
[guest@localhost tmp]$ cat file01.txt
test3
test
test2
[guest@localhost tmp]$ echo "test3" > /tmp/file01.txt
[guest@localhost tmp]$ cat file01.txt
test3
[guest@localhost tmp]$ sudo -i
[root@localhost ~]# chmod -t /tmp
[root@localhost ~]# exit
выход
[guest@localhost tmp]$ ls -l / | grep tmp
drwxrwxrwx. 19 root root 4096 ноя 13 20:17 tmp
[guest@localhost tmp]$ cd /tmp
[guest@localhost tmp]$ echo "test2" >> /tmp/file01.txt
[guest@localhost tmp]$ rm file01.txt
[guest@localhost tmp]$ sudo -i
```

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.