

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Виноградова Варвара Станиславовна НФИбд-01-18

12 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

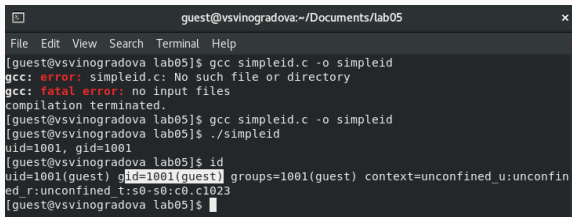
- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться 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@vsvinogradova:~/Documents/lab05
File Edit View Search Terminal Help
[guest@vsvinogradova lab05]$ gcc simpleid.c -o simpleid
gcc: error: simpleid.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[guest@vsvinogradova lab05]$ gcc simpleid.c -o simpleid
[guest@vsvinogradova lab05]$ ./simpleid
uid=1001, gid=1001
[guest@vsvinogradova lab05]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vsvinogradova lab05]$
```

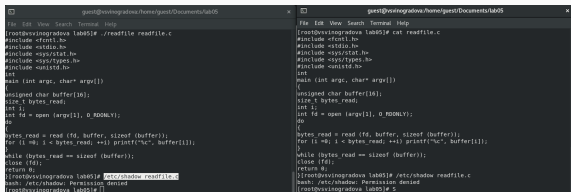
Figure 1: результат программы simpleid

Программа simpleid2

```
guest@vsvinogradova:/home/guest/Documents/lab05
File Edit View Search Terminal Help
[guest@vsvinogradova lab05]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@vsvinogradova lab05]$ su
Password:
[root@vsvinogradova lab05]# chown root:guest /home/guest/simpleid2
chown: cannot access '/home/guest/simpleid2': No such file or directory
[root@vsvinogradova lab05]# chown root:guest /simpleid2
chown: cannot access '/simpleid2': No such file or directory
[root@vsvinogradova lab05]# chown root:guest /home/guest/Documents/lab05/simpleid2
[root@vsvinogradova lab05]# chmod u+s /home/guest/Documents/lab05/simpleid2
[root@vsvinogradova lab05]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@vsvinogradova lab05]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsvinogradova lab05]# chmod g+s /home/guest/Documents/lab05/simpleid2gg
chmod: cannot access '/home/guest/Documents/lab05/simpleid2gg': No such file or directory
[root@vsvinogradova lab05]# chmod u+g simpleid2
[root@vsvinogradova lab05]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 13064 Nov 12 09:42 simpleid2
[root@vsvinogradova lab05]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@vsvinogradova lab05]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vsvinogradova lab05]# chmod g+s simpleid2
[root@vsvinogradova lab05]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 13064 Nov 12 09:42 simpleid2
[root@vsvinogradova lab05]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
```

Figure 2: результат программы simpleid2

Программа readfile

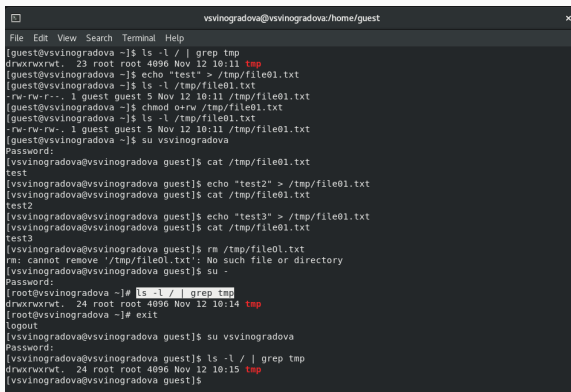


```
guest@vsvinogradova/home/guest/Documents/lab05
File Edit View Search Terminal Help
[root@vsvinogradova lab05]# ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
main (int argc, char* argv[])
{
    unsigned char buffer[10];
    size_t bytes_read;
    int li;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read (fd, buffer, sizeof (buffer));
        for (li = 0; li < bytes_read; ++li) printf("%c", buffer[li]);
        while (bytes_read == sizeof (buffer));
        close (fd);
    }
    return 0;
}
[root@vsvinogradova lab05]# ./etc/shadow readfile.c
bash: ./etc/shadow: Permission denied
[root@vsvinogradova lab05]#

guest@vsvinogradova/home/guest/Documents/lab05
File Edit View Search Terminal Help
[root@vsvinogradova lab05]# 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[10];
    size_t bytes_read;
    int li;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read (fd, buffer, sizeof (buffer));
        for (li = 0; li < bytes_read; ++li) printf("%c", buffer[li]);
        while (bytes_read == sizeof (buffer));
        close (fd);
    }
    return 0;
}
[root@vsvinogradova lab05]# ./etc/shadow readfile.c
bash: ./etc/shadow: Permission denied
[root@vsvinogradova lab05]#
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
vsvinogradova@vsvinogradova:/home/guest
File Edit View Search Terminal Help

[guest@vsvinogradova ~]$ ls -l / | grep tmp
drwxrwxrwt. 23 root root 4096 Nov 12 10:11 tmp
[guest@vsvinogradova ~]$ echo "test" > /tmp/file01.txt
[guest@vsvinogradova ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Nov 12 10:11 /tmp/file01.txt
[guest@vsvinogradova ~]$ chmod o+rw /tmp/file01.txt
[guest@vsvinogradova ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Nov 12 10:11 /tmp/file01.txt
[guest@vsvinogradova ~]$ su vsvinogradova
Password:
[vsvinogradova@vsvinogradova guest]$ cat /tmp/file01.txt
test
[vsvinogradova@vsvinogradova guest]$ echo "test2" > /tmp/file01.txt
[vsvinogradova@vsvinogradova guest]$ cat /tmp/file01.txt
test2
[vsvinogradova@vsvinogradova guest]$ echo "test3" > /tmp/file01.txt
[vsvinogradova@vsvinogradova guest]$ cat /tmp/file01.txt
test3
[vsvinogradova@vsvinogradova guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[vsvinogradova@vsvinogradova guest]$ su -
Password:
[root@vsvinogradova ~]# ls -l / | grep tmp
drwxrwxrwt. 24 root root 4096 Nov 12 10:14 tmp
[root@vsvinogradova ~]# exit
logout
[vsvinogradova@vsvinogradova guest]$ su vsvinogradova
Password:
[vsvinogradova@vsvinogradova guest]$ ls -l / | grep tmp
drwxrwxrwt. 24 root root 4096 Nov 12 10:15 tmp
[vsvinogradova@vsvinogradova guest]$
```

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.