

# Презентация по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

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.



```
simpleid.c  [-M--]  0 L: [ 1+ 3  4/ 12]  *(62 / 175b) 0010 0x00A  [*] [X]
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

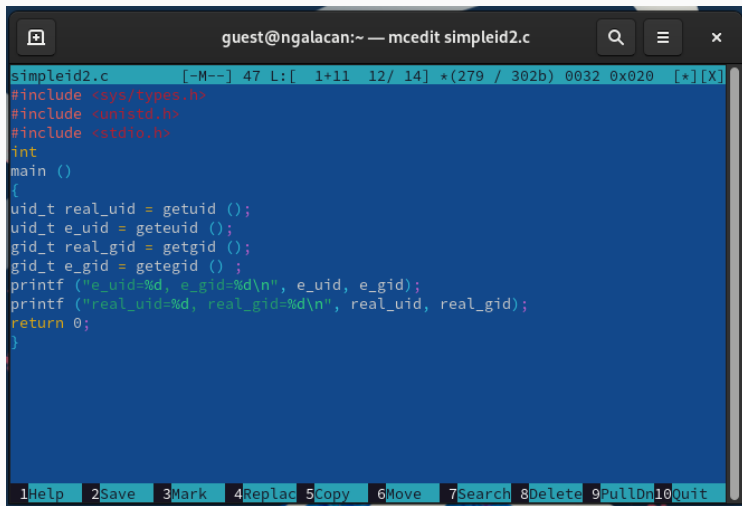
int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Рис. 1: Программа simpleid.c

## Выполнение лабораторной работы

```
[guest@ngalacan ~]$ gcc simpleid.c -o simpleid
[guest@ngalacan ~]$ ls -l
total 32
drwxrwxrwx. 2 guest users   19 Mar 18 11:19 dir1
drwxr-xr-x. 2 guest users    6 Sep 13  2023 Documents
drwxr-xr-x. 2 guest users    6 Sep 13  2023 Pictures
-rwxr-xr-x. 1 guest users 25960 Mar 31 14:08 simpleid
-rw-r--r--. 1 guest users   175 Mar 31 14:07 simpleid.c
[guest@ngalacan ~]$ ./simpleid
uid=1004, gid=100
[guest@ngalacan ~]$ id
uid=1004(guest) gid=100(users) groups=100(users),1005(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ngalacan ~]$
```

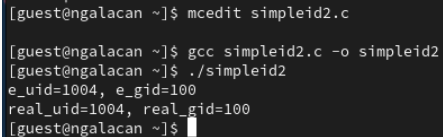
Рис. 2: Компиляция и выполнение. Сравнение с id



```
simpleid2.c      [-M--] 47 L:[ 1+11 12/ 14] *(279 / 302b) 0032 0x020 [*] [X]
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t real_uid = getuid ();
uid_t e_uid = geteuid ();
gid_t real_gid = getgid ();
gid_t e_gid = getegid ();
printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
return 0;
}
```

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit

Рис. 3: Программа simpleid2.c



```
[guest@ngalacan ~]$ mcedit simpleid2.c  
  
[guest@ngalacan ~]$ gcc simpleid2.c -o simpleid2  
[guest@ngalacan ~]$ ./simpleid2  
e_uid=1004, e_gid=100  
real_uid=1004, real_gid=100  
[guest@ngalacan ~]$
```

Рис. 4: Компиляция и выполнение

```
real_uid=1004, real_gid=100
[guest@ngalacan ~]$ su -
Password:
[root@ngalacan ~]# chown root:guest /home/guest/simpleid2
[root@ngalacan ~]# chmod u+s /home/guest/simpleid2
[root@ngalacan ~]# exit
logout
[guest@ngalacan ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Mar 31 14:10 simpleid2
[guest@ngalacan ~]$ ./simpleid2
e_uid=0, e_gid=100
real_uid=1004, real_gid=100
[guest@ngalacan ~]$ id
uid=1004(guest) gid=100(users) groups=100(users),1005(guest) context=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ngalacan ~]$
```

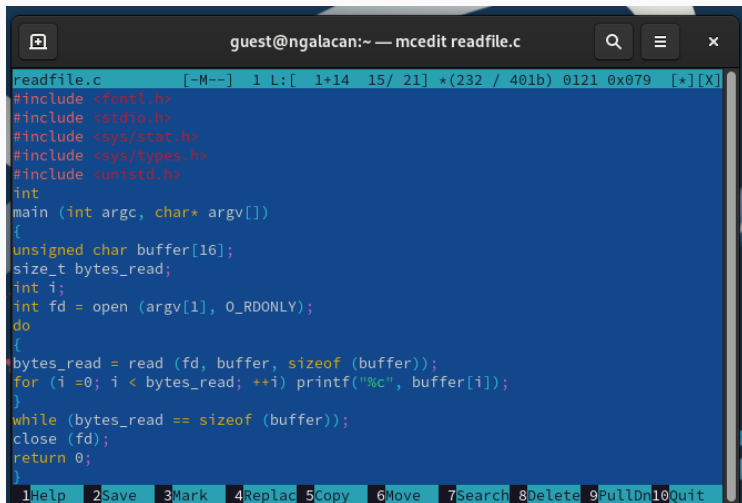
Рис. 5: Запуск simpleid2 с SetUID. Сравнение результатов



## Выполнение лабораторной работы

```
[guest@ngalacan ~]$ su -
Password:
[root@ngalacan ~]# chmod u-s /home/guest/simpleid2
[root@ngalacan ~]# chmod g+s /home/guest/simpleid2
[root@ngalacan ~]# exit
logout
[guest@ngalacan ~]$ ls -l
total 64
drwxrwxrwx. 2 guest users 19 Mar 18 11:19 dir1
drwxr-xr-x. 2 guest users 6 Sep 13 2023 Documents
drwxr-xr-x. 2 guest users 6 Sep 13 2023 Pictures
-rwxr-xr-x. 1 guest users 25960 Mar 31 14:08 simpleid
-rwxr-sr-x. 1 root guest 26064 Mar 31 14:10 simpleid2
-rw-r--r--. 1 guest users 302 Mar 31 14:10 simpleid2.c
-rw-r--r--. 1 guest users 175 Mar 31 14:07 simpleid.c
[guest@ngalacan ~]$ ./simpleid2
e_uid=1004, e_gid=1005
real_uid=1004, real_gid=100
[guest@ngalacan ~]$
```

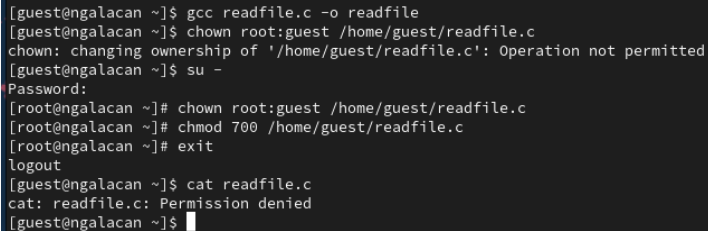
Рис. 6: Запуск simpleid2 с SetGID. Сравнение результатов



```
readfile.c      [-M--]  1 L:[  1+14  15/ 21] *(232 / 401b) 0121 0x079  [*][X]
#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;
}
```

1 Help 2 Save 3 Mark 4 Replac 5 Copy 6 Move 7 Search 8 Delete 9 PullDn 10 Quit

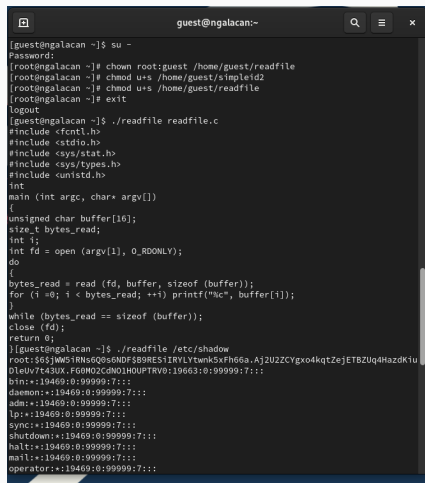
Рис. 7: Программа readfile.c



```
[guest@ngalacan ~]$ gcc readfile.c -o readfile
[guest@ngalacan ~]$ chown root:guest /home/guest/readfile.c
chown: changing ownership of '/home/guest/readfile.c': Operation not permitted
[guest@ngalacan ~]$ su -
Password:
[root@ngalacan ~]# chown root:guest /home/guest/readfile.c
[root@ngalacan ~]# chmod 700 /home/guest/readfile.c
[root@ngalacan ~]# exit
logout
[guest@ngalacan ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@ngalacan ~]$
```

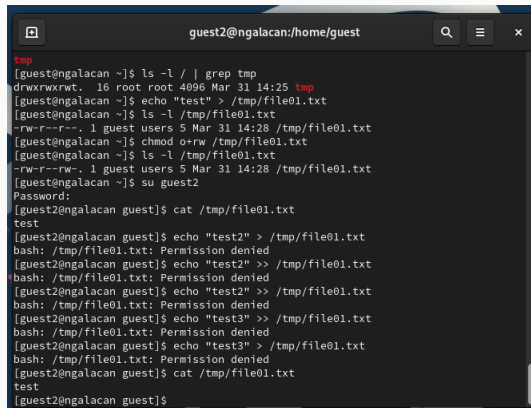
Рис. 8: Изменение прав доступа, проверка от имени пользователя guest

# Выполнение лабораторной работы



```
guest@ngalacan:~  
[guest@ngalacan ~]$ su -  
Password:  
[root@ngalacan ~]# chown root:guest /home/guest/readfile  
[root@ngalacan ~]# chmod u+s /home/guest/simpleid2  
[root@ngalacan ~]# chmod u+s /home/guest/readfile  
[root@ngalacan ~]# exit  
logout  
[guest@ngalacan ~]$ ./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[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;  
}[guest@ngalacan ~]$ ./readfile /etc/shadow  
root:$6$jWMS1RNs6Qs6NDF$B9RES1IRLYtwnk5xFh66a.Aj2U2ZCYgx04kqtZeJTBZUq4HzdKiU  
DLeUv7t43UX.FG0M02CdNO1HOUPTRV0:19663:0:99999:7::  
bin:*.19469:0:99999:7::  
daemon:*.19469:0:99999:7::  
adm:*.19469:0:99999:7::  
lp:*.19469:0:99999:7::  
sync:*.19469:0:99999:7::  
shutdown:*.19469:0:99999:7::  
halt:*.19469:0:99999:7::  
mail:*.19469:0:99999:7::  
operator:*.19469:0:99999:7::
```

Рис. 9: Установка SetUID для readfile и проверка

A terminal window titled 'guest2@ngalacan:/home/guest' with search, menu, and close icons. It shows a series of commands to create a file, change permissions, and attempt to write to it. The file '/tmp/file01.txt' is created with permissions 'drwxrwxrwt.' and owned by 'root'. It is then changed to '-rw-r--r--' and owned by 'guest'. The user 'guest2' switches to 'guest' and attempts to write to the file, but all attempts are denied due to permissions.

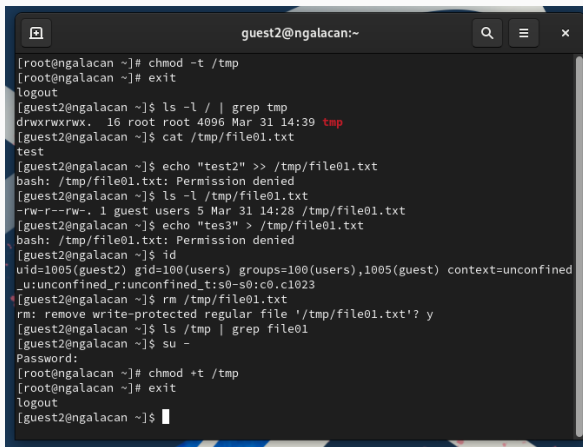
```
tmp
[guest2@ngalacan ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Mar 31 14:25 tmp
[guest2@ngalacan ~]$ echo "test" > /tmp/file01.txt
[guest2@ngalacan ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest users 5 Mar 31 14:28 /tmp/file01.txt
[guest2@ngalacan ~]$ chmod o+rw /tmp/file01.txt
[guest2@ngalacan ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest users 5 Mar 31 14:28 /tmp/file01.txt
[guest2@ngalacan ~]$ su guest2
Password:
[guest2@ngalacan guest]$ cat /tmp/file01.txt
test
[guest2@ngalacan guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ngalacan guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ngalacan guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ngalacan guest]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ngalacan guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@ngalacan guest]$ cat /tmp/file01.txt
test
[guest2@ngalacan guest]$
```

Рис. 10: Создание файла, изменение прав, просмотр и попытки записи

```
rm: remove write-protected regular file '/tmp/file01.txt'? n  
[guest2@ngalacan ~]$ rm /tmp/file01.txt  
rm: remove write-protected regular file '/tmp/file01.txt'? y  
rm: cannot remove '/tmp/file01.txt': Operation not permitted  
[guest2@ngalacan ~]$
```

Рис. 11: Попытка удаления

## Выполнение лабораторной работы



```
guest2@ngalacan:~  
[root@ngalacan ~]# chmod -t /tmp  
[root@ngalacan ~]# exit  
logout  
[guest2@ngalacan ~]$ ls -l / | grep tmp  
drwxrwxrwx. 16 root root 4096 Mar 31 14:39 tmp  
[guest2@ngalacan ~]$ cat /tmp/file01.txt  
test  
[guest2@ngalacan ~]$ echo "test2" >> /tmp/file01.txt  
bash: /tmp/file01.txt: Permission denied  
[guest2@ngalacan ~]$ ls -l /tmp/file01.txt  
-rw-r--rw-. 1 guest users 5 Mar 31 14:28 /tmp/file01.txt  
[guest2@ngalacan ~]$ echo "tes3" > /tmp/file01.txt  
bash: /tmp/file01.txt: Permission denied  
[guest2@ngalacan ~]$ id  
uid=1005(guest2) gid=100(users) groups=100(users),1005(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@ngalacan ~]$ rm /tmp/file01.txt  
rm: remove write-protected regular file '/tmp/file01.txt'? y  
[guest2@ngalacan ~]$ ls /tmp | grep file01  
[guest2@ngalacan ~]$ su -  
Password:  
[root@ngalacan ~]# chmod +t /tmp  
[root@ngalacan ~]# exit  
logout  
[guest2@ngalacan ~]$
```

Рис. 12: Повторение операций без атрибута t

Были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрены работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.