

Презентация по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Танрибергенов Э.

2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Танрибергенов Эльдар
- студент 4 курса из группы НПИбд-02-21
- ФМиЕН, кафедра прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Цели и задачи

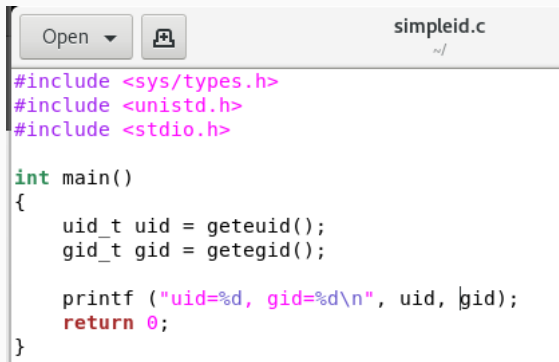
Изучение механизмов изменения идентификаторов, применения *SetUID*- и *Sticky*-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита *Sticky* на запись и удаление файлов.

- Исследовать *SetUID*- и *SetGID*-биты;
- Исследовать *Sticky*-бит.

Результаты

Исследование *SetUID*- и *SetGID*-битов

- Программа выводит *UID* и *GID* владельца файла
- Программа написана на C



```
simpleid.c
~|

#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main()
{
    uid_t uid = geteuid();
    gid_t gid = getegid();

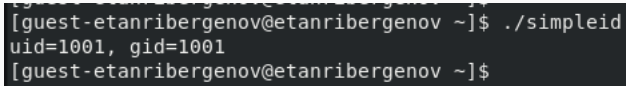
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Рис. 1: Программа, выводящая UID и GID

- команда *gcc <file.c>*

```
[guest-etanribergenov@etanribergenov ~]$ gedit simpleid.c
[guest-etanribergenov@etanribergenov ~]$ gcc simpleid.c -o simpleid
[guest-etanribergenov@etanribergenov ~]$ ls | grep -i "simpleid"
simpleid
simpleid.c
[guest-etanribergenov@etanribergenov ~]$
```

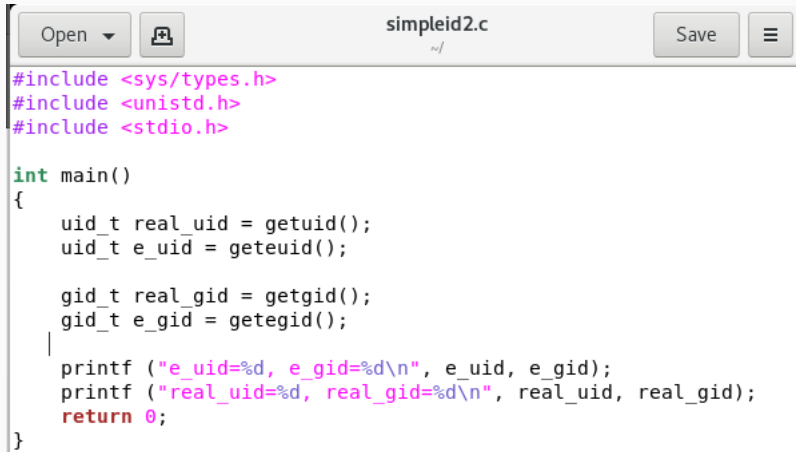
Рис. 2: Компилирование программы



```
[guest-etanribergenov@etanribergenov ~]$ ./simpleid  
uid=1001, gid=1001  
[guest-etanribergenov@etanribergenov ~]$
```

Рис. 3: Выполнение программы

Исследование *SetUID*- и *SetGID*-битов



```
Open  [icon] simpleid2.c  Save  [menu]  
#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;  
}
```

Рис. 4: Добавление в программу действительных идентификаторов

```
[guest-etanribergenov@etanribergenov ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest-etanribergenov@etanribergenov ~]$ █
```

Рис. 5: Запуск программы

Исследование *SetUID*- и *SetGID*-битов

- ***chown*** - меняет владельца файла/директории
- ***chmod*** - меняет атрибуты файла/директории
- ***u+s*** - устанавливает SetUID на файл/директорию

```
[guest-etanribergenov@etanribergenov ~]$ su etanribergenov
Password:
[etanribergenov@etanribergenov guest-etanribergenov]$ sudo su
[sudo] password for etanribergenov:
[root@etanribergenov guest-etanribergenov]# chown root:guest-etanribergenov
/home/guest-etanribergenov/simpleid2
[root@etanribergenov guest-etanribergenov]# chmod u+s /home/guest-etanribergenov/simpleid2
[root@etanribergenov guest-etanribergenov]#
```

Рис. 6: Смена владельца файла и добавление SetUID-бита

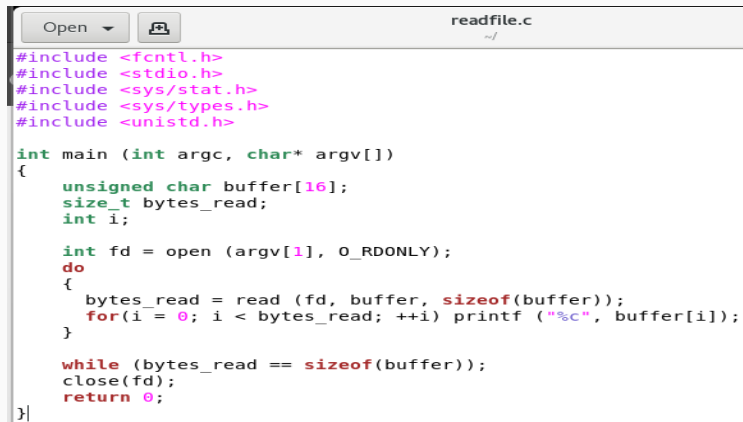
```
[guest-etanribergenov@etanribergenov ~]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest-etanribergenov 18312 Nov 15 20:19 simpleid2  
[guest-etanribergenov@etanribergenov ~]$
```

Рис. 7: Проверка добавления SUID-бита

```
[guest-etanribergenov@etanribergenov ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest-etanribergenov@etanribergenov ~]$
```

Рис. 8: Запуск программы simpleid2

Исследование *SetUID*- и *SetGID*-битов



```
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;
}
```

Рис. 9: Программа, считывающая и выводящая в консоль содержимое файла

- ***chown*** - меняет владельца файла/директории
- ***chmod*** - меняет атрибуты файла/директории

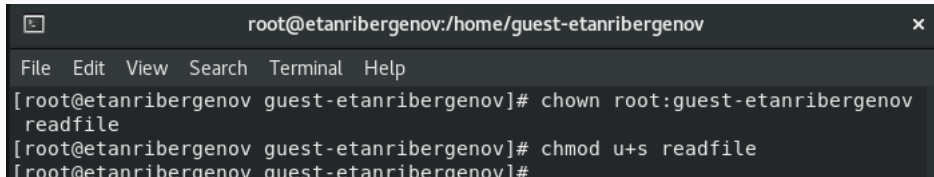
```
[root@etanribergenov guest-etanribergenov]# chown root:guest-etanribergenov  
readfile.c  
[root@etanribergenov guest-etanribergenov]# chmod 700 readfile.c  
[root@etanribergenov guest-etanribergenov]#
```

Рис. 10: Смена владельца файла и разрешение только суперпользователю читать его

```
[guest-etanribergenov@etanribergenov ~]$ cat readfile.c  
cat: readfile.c: Permission denied
```

Рис. 11: Проверка невозможности чтения файла пользователем guest-etanribergenov

- ***chown*** - меняет владельца файла/директории
- ***chmod*** - меняет атрибуты файла/директории
- ***u+s*** - устанавливает SetUID на файл/директорию

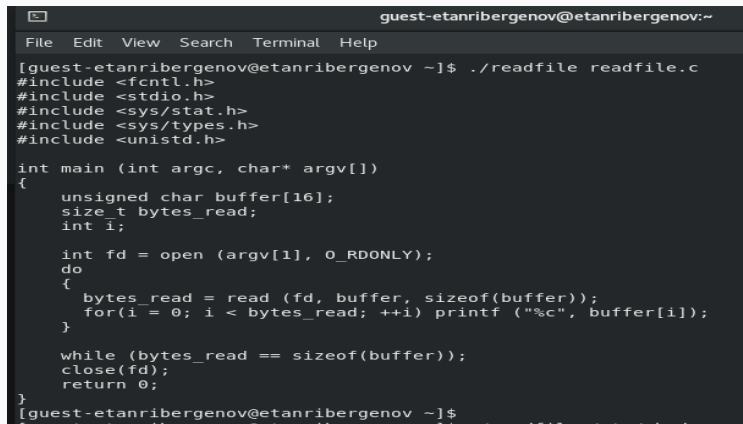


```
root@etanribergenov:/home/guest-etanribergenov
File Edit View Search Terminal Help
[root@etanribergenov guest-etanribergenov]# chown root:guest-etanribergenov readfile
[root@etanribergenov guest-etanribergenov]# chmod u+s readfile
[root@etanribergenov guest-etanribergenov]#
```

Рис. 12: Смена владельца у программы `readfile` и установка SetUID-бита

Исследование *SetUID*- и *SetGID*-битов

- Программа читает этот файл, т.к. инициатор (владелец) программы - суперпользователь *root*

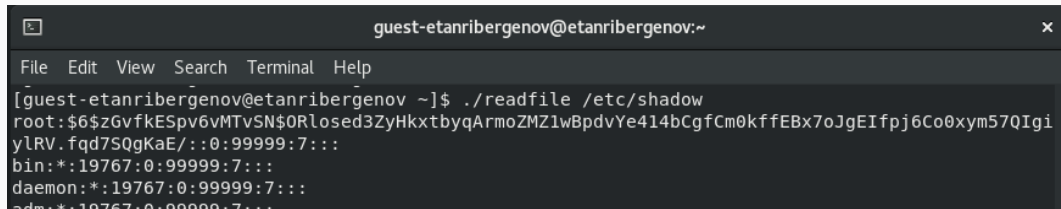


```
guest-etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[guest-etanribergenov@etanribergenov ~]$ ./readfile readfile.c  
#include <fcntl.h>  
#include <stdio.h>  
#include <sys/stat.h>  
#include <sys/types.h>  
#include <unistd.h>  
  
int main (int argc, char* argv[])  
{  
    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-etanribergenov@etanribergenov ~]$
```

Рис. 13: Проверка возможности чтения программой *readfile* другого файла

Исследование *SetUID*- и *SetGID*-битов

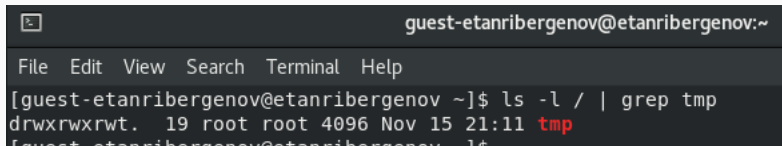
- Программа читает этот файл, т.к. инициатор (владелец) программы - суперпользователь *root*



```
guest-etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[guest-etanribergenov@etanribergenov ~]$ ./readfile /etc/shadow  
root:$6$zGvfkESpv6vMTvSN$0Rlosed3ZyHkxtbyqArmoZMZlwBpdvYe414bCgfCm0kffEBx7oJgEIfpj6Co0xym57QIgi  
ylRV.fqd7SQgKaE/::0:99999:7:::  
bin:*:19767:0:99999:7:::  
daemon:*:19767:0:99999:7:::  
adm:*:19767:0:99999:7:::
```

Рис. 14: Проверка возможности чтения программой readfile файла */etc/shadow*

- “*t*” в атрибутах файла/директории говорит о наличии *Sticky*-бита



```
guest-etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[guest-etanribergenov@etanribergenov ~]$ ls -l / | grep tmp  
drwxrwxrwt. 19 root root 4096 Nov 15 21:11 tmp
```

Рис. 15: Проверка наличия *Sticky*-бита на директории /tmp

```
[guest-etanribergenov@etanribergenov ~]$ echo "test" > /tmp/file01-etanribergenov.txt  
[guest-etanribergenov@etanribergenov ~]$
```

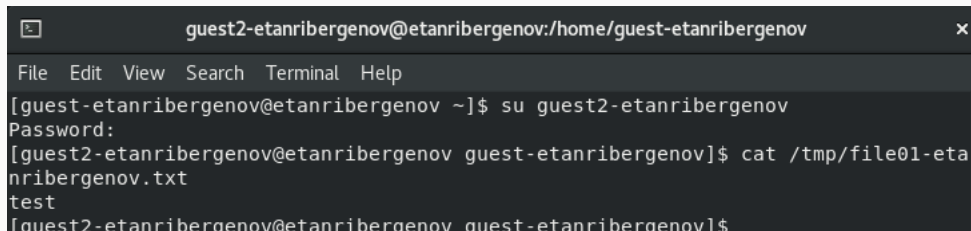
Рис. 16: Создание файла со словом «test» в директории /tmp от имени пользователя guest-etanribergenov

- ***chmod*** - меняет атрибуты файла/директории
- “***o+***” - задаёт права доступа для категории пользователей “*все остальные*”

```
[guest-etanribergenov@etanribergenov ~]$ ls -l /tmp/file01-etanribergenov.txt
-rw-rw-r--. 1 guest-etanribergenov guest-etanribergenov 5 Nov 15 21:29 /tmp/file01-etanribergenov.txt
[guest-etanribergenov@etanribergenov ~]$ chmod o+rw /tmp/file01-etanribergenov.txt
[guest-etanribergenov@etanribergenov ~]$ ls -l /tmp/file01-etanribergenov.txt
-rw-rw-rw-. 1 guest-etanribergenov guest-etanribergenov 5 Nov 15 21:29 /tmp/file01-etanribergenov.txt
```

Рис. 17: Просмотр атрибутов и разрешение на чтение и запись для категории пользователей «остальные»

- ***su <user>*** - ВХОД В СИСТЕМУ ОТ ИМЕНИ ПОЛЬЗОВАТЕЛЯ *user*



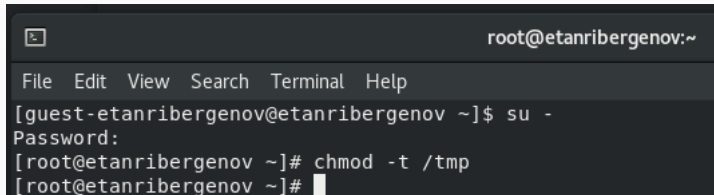
```
guest2-etanribergenov@etanribergenov:/home/guest-etanribergenov
File Edit View Search Terminal Help
[guest-etanribergenov@etanribergenov ~]$ su guest2-etanribergenov
Password:
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$ cat /tmp/file01-etanribergenov.txt
test
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$
```

Рис. 18: Попытка чтения файла пользователем, не являющимся его владельцем

```
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$  
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$ rm /tmp/file01-etanribergenov.txt  
rm: cannot remove '/tmp/file01-etanribergenov.txt': Operation not permitted  
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$
```

Рис. 19: Попытка удаления файла пользователем, не являющимся его владельцем

- ***chmod*** - меняет атрибуты файла/директории
- ***-t*** - убирает Sticky-бит из атрибутов файла/директории



```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[guest-etanribergenov@etanribergenov ~]$ su -  
Password:  
[root@etanribergenov ~]# chmod -t /tmp  
[root@etanribergenov ~]#
```

Рис. 20: Снятие Sticky-бита с директории /tmp суперпользователем

- Удаление возможно после снятия атрибута *t*

```
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$ echo "test5" > /tmp  
/file01-etanribergenov.txt  
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$  
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$ rm /tmp/file01-etan  
ribergenov.txt  
[guest2-etanribergenov@etanribergenov guest-etanribergenov]$
```

Рис. 21: Попытка удаления файла пользователем, не являющимся его владельцем

Вывод

В результате выполнения работы я изучил механизмы изменения идентификаторов, применения *SetUID*- и *Sticky*-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита *Sticky* на запись и удаление файлов.