

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Хусаинова Д.А. Группа НПИбд-02-21

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.

Теоретическое введение 1/2

. Дополнительные атрибуты файлов Linux

В Linux существует три основных вида прав — право на чтение (read), запись (write) и выполнение (execute), а также три категории пользователей, к которым они могут применяться — владелец файла (user), группа владельца (group) и все остальные (others). Но, кроме прав чтения, выполнения и записи, есть еще три дополнительных атрибута. [a]

Sticky bit

Используется в основном для каталогов, чтобы защитить в них файлы. В такой каталог может писать любой пользователь. Но, из такой директории пользователь может удалить только те файлы, владельцем ^{3/19}

SUID (Set User ID)

Атрибут исполняемого файла, позволяющий запустить его с правами владельца. В Linux приложение запускается с правами пользователя, запустившего указанное приложение. Это обеспечивает дополнительную безопасность т.к. процесс с правами пользователя не сможет получить доступ к важным системным файлам, которые принадлежат пользователю root.

SGID (Set Group ID)

Аналогичен suid, но относиться к группе. Если установить sgid для каталога, то все файлы созданные в нем, при запуске будут принимать идентификатор группы каталога, а не группы владельца, который

Выполнение лабораторной работы

```
[guest1@dakhusainova ~]$ touch simplified.c  
[guest1@dakhusainova ~]$ mcedit simplified.c
```

Рис. 1: Создание файла

Компиляция simpleid.c

```
[guest1@dakhusainova ~]$ gcc simplified.c -o simplified
[guest1@dakhusainova ~]$ ls
Desktop  Documents  Music      Public    simplified.c  Videos
dir1     Downloads  Pictures   simplified  Templates
```

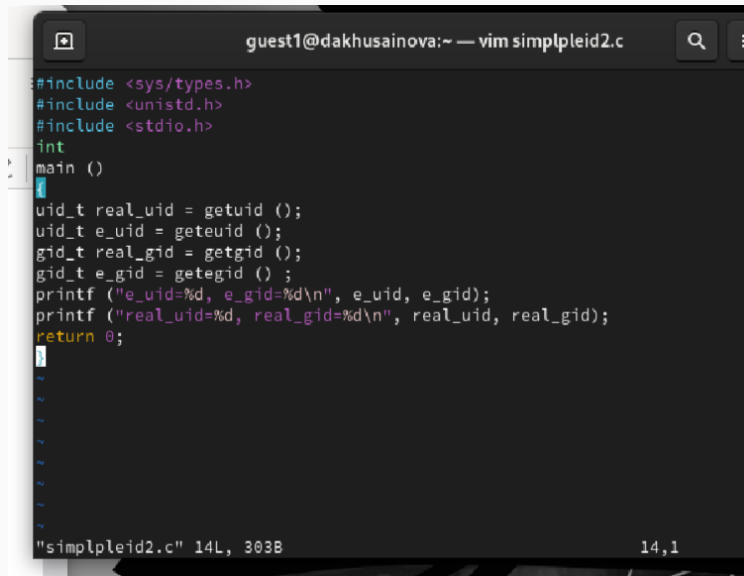
Рис. 2: Компиляция

Сравнения вывода команды и кода из файла

```
[guest1@dakhusainova ~]$ ./simplified  
uid=1003, gid=1003  
[guest1@dakhusainova ~]$ id  
uid=1003(guest1) gid=1003(guest1) groups=1003(guest1) context=unconfined_u:unc
```

Рис. 3: Сравнения вывода команды и кода из файла

Изменение кода программы



The image shows a terminal window with the vim editor open. The title bar indicates the user is 'guest1@dakhusainova' and the file being edited is 'vim simplpleid2.c'. The code in the editor is a C program that includes standard headers and prints user and group IDs. The status bar at the bottom shows the file path and line/column information: '"simplpleid2.c" 14L, 303B' and '14,1'.

```
guest1@dakhusainova:~ — vim simplpleid2.c

#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;
}

"simplpleid2.c" 14L, 303B 14,1
```

```
[root@dakhusainova guest1]# gcc simplpleid2.c -o simpleid2  
[root@dakhusainova guest1]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@dakhusainova guest1]#
```

Рис. 5: Компиляция и запуск программы

От имени суперпользователя команды

```
[root@dakhusainova guest1]# chown root:guest /home/guest1/simpleid2  
[root@dakhusainova guest1]# chmod u+s /home/guest1/simpleid2  
[root@dakhusainova guest1]#
```

Рис. 6: От имени суперпользователя команды

Сравнение вывода simpleid2 и команды id

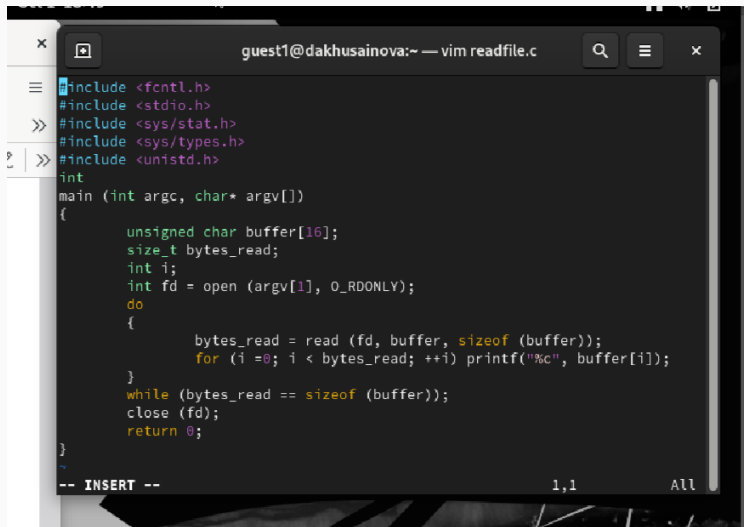
```
[root@dakhusainova guest1]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 17720 Oct  1 18:39 simpleid2
[root@dakhusainova guest1]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@dakhusainova guest1]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@dakhusainova guest1]#
```

Рис. 7: simpleid2 и id

```
[root@dakhusainova guest1]# sudo id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@dakhusainova guest1]# su guest1
[guest1@dakhusainova ~]$ id
uid=1003(guest1) gid=1003(guest1) groups=1003(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@dakhusainova ~]$
```

Рис. 8: SetGID-бит

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;
}
```

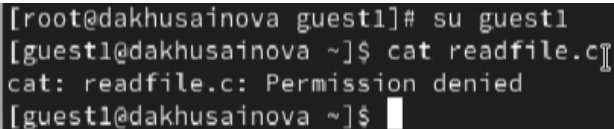
-- INSERT --

1,1 All

```
[root@dakhusainova guest1]# sudo chmod 700 /home/guest/dir1  
[root@dakhusainova guest1]# sudo chmod 700 /home/guest1/readfile.c  
[root@dakhusainova guest1]# sudo chmod -r /home/guest1/readfile.c  
[root@dakhusainova guest1]# sudo chmod u+s /home/guest1/readfile.c  
[root@dakhusainova guest1]#
```

Рис. 9: Изменение прав

Проверка возможности чтение файла



```
[root@dakhusainova guest1]# su guest1
[guest1@dakhusainova ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest1@dakhusainova ~]$
```

Рис. 10: Проверка возможности чтение файла

Исследование Sticky-бита

```
guest2@dakhusainova:/home/guest1
[guest1@dakhusainova ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Oct 1 18:52 tmp
[guest1@dakhusainova ~]$ echo "test" > /tmp/file01.txt
[guest1@dakhusainova ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest1 guest1 5 Oct 1 18:57 /tmp/file01.txt
[guest1@dakhusainova ~]$ chmod o+rw /tmp/file01.txt
[guest1@dakhusainova ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest1 guest1 5 Oct 1 18:57 /tmp/file01.txt
[guest1@dakhusainova ~]$ su guest2
Password:
[guest2@dakhusainova guest1]$ cat /tmp/file01.txt
test
[guest2@dakhusainova guest1]$ echo "test2" > /tmp/file01.txt
[guest2@dakhusainova guest1]$ cat /tmp/file01.txt
test2
[guest2@dakhusainova guest1]$ echo "test3" > /tmp/file01.txt
[guest2@dakhusainova guest1]$ cat /tmp/file01.txt
test3
[guest2@dakhusainova guest1]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dakhusainova guest1]$ su -
Password:
[root@dakhusainova ~]# chmod -t /tmp
[root@dakhusainova ~]# exit
logout
[guest2@dakhusainova guest1]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 Oct 1 19:00 tmp
[guest2@dakhusainova guest1]$ echo "test2" > /tmp/file01.txt
[guest2@dakhusainova guest1]$ cat /tmp/file01.txt
test2
[guest2@dakhusainova guest1]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dakhusainova guest1]$ su -
Password:
[root@dakhusainova ~]# chmod +t /tmp
[root@dakhusainova ~]# exit
logout
[guest2@dakhusainova guest1]$
```

Изучили механизм изменения идентификаторов, применила SetUID- и Sticky-биты. Получила практические навыки работы в кон- соли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа:

<https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Группы пользователей: [https://losst.pro/gruppy-polzovatelej-](https://losst.pro/gruppy-polzovatelej-linux#%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%)

[linux#%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%](https://losst.pro/gruppy-polzovatelej-linux#%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%)