

Лабораторная работа №5

Основы информационной безопасности

Волгин И. А.

12 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

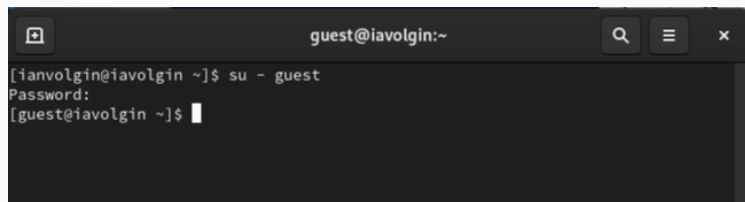
- Волгин Иван Алексеевич
- Студент по программе “Компьютерные и информационные науки”
- Российский университет дружбы народов

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

Setuid, Setgid и Sticky Bit - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги.

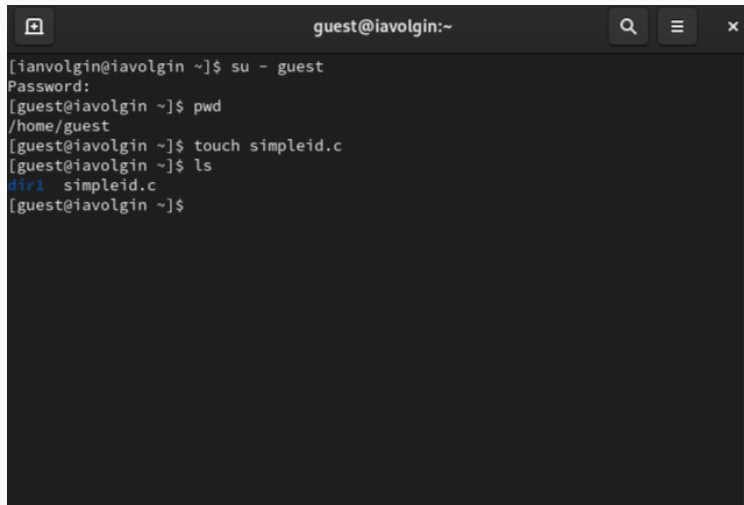
Подготовка к выполнению работы. Проверка установки ПО

```
[ianvolgin@iavolgin ~]$ yum install gcc
Error: This command has to be run with superuser privileges (under the root use
r on most systems).
[ianvolgin@iavolgin ~]$ sudo yum install gcc
[sudo] password for ianvolgin:
Last metadata expiration check: 1:59:06 ago on Thu 11 Apr 2024 02:41:35 PM MSK.
Package gcc-11.4.1-2.1.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ianvolgin@iavolgin ~]$ setenforce 0
setenforce: security_setenforce() failed: Permission denied
[ianvolgin@iavolgin ~]$ sudo setenforce 0
[ianvolgin@iavolgin ~]$ getenforce
Permissive
[ianvolgin@iavolgin ~]$
[ianvolgin@iavolgin ~]$
```



```
guest@iavolgin:~  
[ianvolgin@iavolgin ~]$ su - guest  
Password:  
[guest@iavolgin ~]$
```

Создание программы simpleid.c.



```
guest@iavolgin:~  
[ianvolgin@iavolgin ~]$ su - guest  
Password:  
[guest@iavolgin ~]$ pwd  
/home/guest  
[guest@iavolgin ~]$ touch simpleid.c  
[guest@iavolgin ~]$ ls  
dir1 simpleid.c  
[guest@iavolgin ~]$
```


Заполнение программы simpleid.c

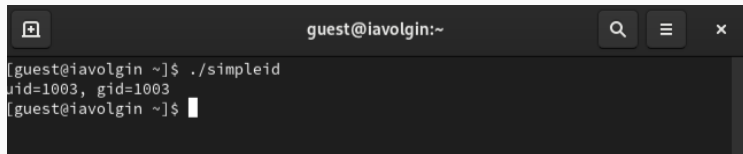


```
GNU nano 5.6.1 simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

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

[Read 12 lines]

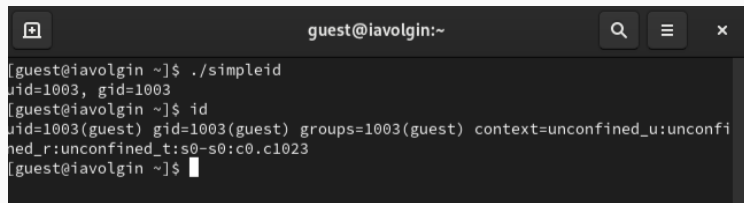
^G Help **^O** Write Out **^W** Where Is **^K** Cut **^T** Execute
^X Exit **^R** Read File **^I** Replace **^U** Paste **^J** Justify



A terminal window titled "guest@iavolgin:~" with standard window controls (minimize, maximize, close) on the right. The terminal shows the execution of the command `./simpleid`, which outputs `uid=1003, gid=1003`. The prompt returns to `[guest@iavolgin ~]$` with a cursor.

```
[guest@iavolgin ~]$ ./simpleid
uid=1003, gid=1003
[guest@iavolgin ~]$
```

Команда id, сравнение результатов

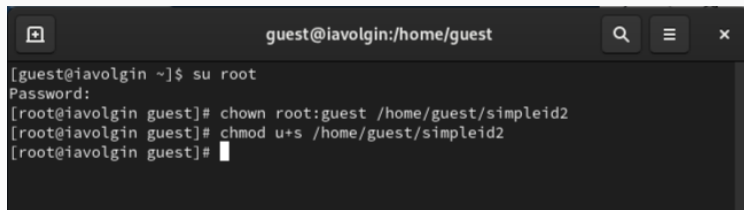


```
guest@iavolgin:~  
[guest@iavolgin ~]$ ./simpleid  
uid=1003, gid=1003  
[guest@iavolgin ~]$ id  
uid=1003(guest) gid=1003(guest) groups=1003(guest) context=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@iavolgin ~]$
```

Компиляция и запуск программы simpleid2.c

```
[guest@iavolgin ~]$ gcc simpleid2.c -o simpleid2  
[guest@iavolgin ~]$ ./simpleid2  
e_uid=1003, e_gid=1003  
real_uid=1003, real_gid=1003  
[guest@iavolgin ~]$
```

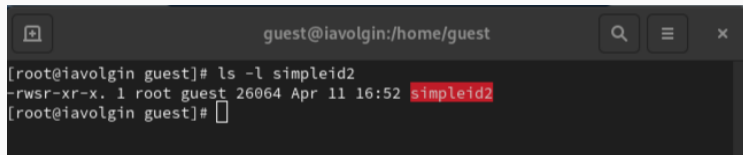
Поменял владельца программы simpleid2.



```
guest@iavolgin:/home/guest
[guest@iavolgin ~]$ su root
Password:
[root@iavolgin guest]# chown root:guest /home/guest/simpleid2
[root@iavolgin guest]# chmod u+s /home/guest/simpleid2
[root@iavolgin guest]#
```

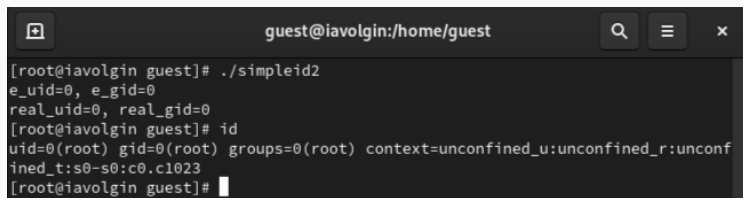
The image shows a terminal window with a dark background. The title bar at the top reads 'guest@iavolgin:/home/guest' and includes standard window controls (minimize, maximize, close). The terminal content shows a user switching from 'guest' to 'root' using 'su root'. After entering the password, the user runs two commands: 'chown root:guest /home/guest/simpleid2' and 'chmod u+s /home/guest/simpleid2'. The prompt returns to '[root@iavolgin guest]#' after each command, with a cursor visible at the end of the final line.

Выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2.



```
guest@iavolgin:/home/guest
[root@iavolgin guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Apr 11 16:52 simpleid2
[root@iavolgin guest]#
```

Сравнение результатов simpleid2 и id.



```
guest@iavolgin:/home/guest
[root@iavolgin guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@iavolgin guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@iavolgin guest]#
```

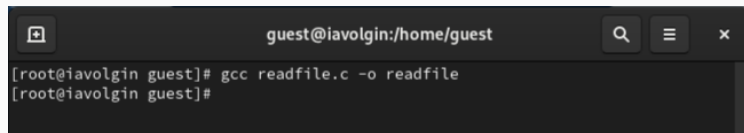
Создание программы readfile.c.



The screenshot shows a terminal window with the nano text editor. The title bar indicates the user is 'guest' at 'iavolgin:/home/guest'. The editor is editing a file named 'readfile.c'. The code is as follows:

```
GNU nano 5.6.1      readfile.c      Modified
#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;
}
```

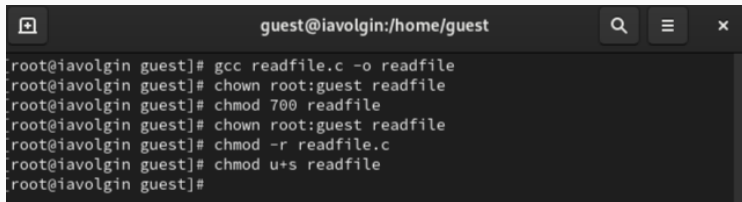

Компиляция программы readfile.c.



A terminal window with a dark background. The title bar at the top shows a window icon, the text "guest@iavolgin:/home/guest", and search, menu, and close buttons. The terminal content shows a root user at the iavolgin guest machine. The command "gcc readfile.c -o readfile" has been entered and executed, resulting in a new prompt line.

```
guest@iavolgin:/home/guest  
[root@iavolgin guest]# gcc readfile.c -o readfile  
[root@iavolgin guest]#
```

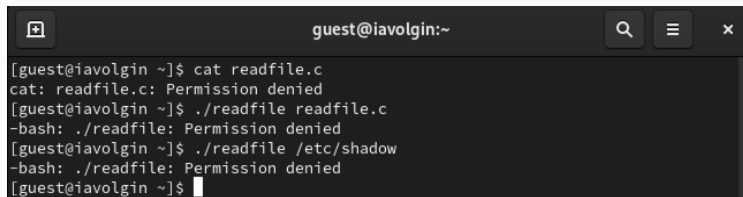
Смена владельца файла readfile.c.

A terminal window with a dark background and light text. The title bar at the top reads 'guest@iavolgin:/home/guest' and includes search, menu, and close icons. The terminal shows a series of commands and their outputs, all starting with 'root@iavolgin guest]#'. The commands are: 'gcc readfile.c -o readfile', 'chown root:guest readfile', 'chmod 700 readfile', 'chown root:guest readfile', 'chmod -r readfile.c', and 'chmod u+s readfile'. The prompt returns after each command.

```
root@iavolgin guest]# gcc readfile.c -o readfile
root@iavolgin guest]# chown root:guest readfile
root@iavolgin guest]# chmod 700 readfile
root@iavolgin guest]# chown root:guest readfile
root@iavolgin guest]# chmod -r readfile.c
root@iavolgin guest]# chmod u+s readfile
root@iavolgin guest]#
```

Figure 1: Смена владельца

Проверка правильности изменений



```
guest@iavolgin:~  
[guest@iavolgin ~]$ cat readfile.c  
cat: readfile.c: Permission denied  
[guest@iavolgin ~]$ ./readfile readfile.c  
-bash: ./readfile: Permission denied  
[guest@iavolgin ~]$ ./readfile /etc/shadow  
-bash: ./readfile: Permission denied  
[guest@iavolgin ~]$
```

Я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.
Получение практических навыков работы в консоли с дополнительными атрибутами.