

Лабораторная работа №5

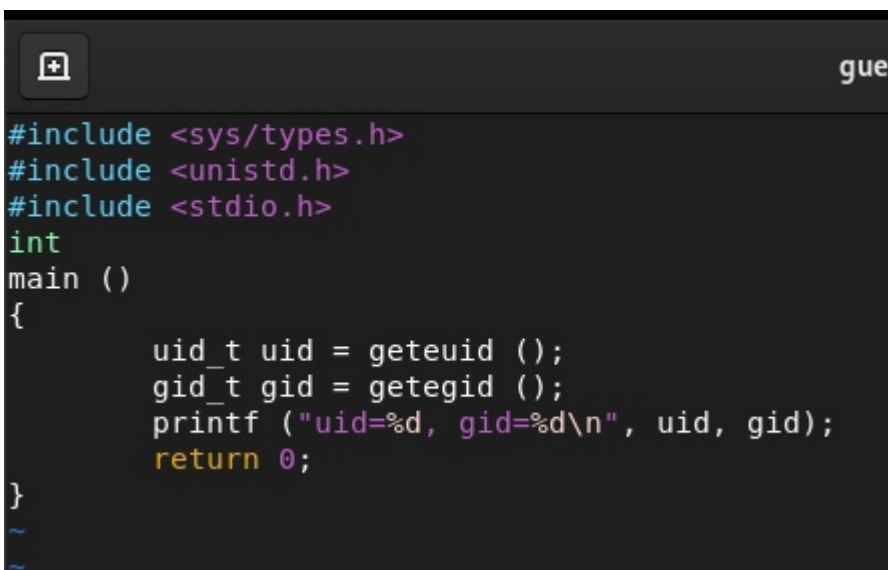
Уваров Илья НПИбд-02-19

Цель 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.

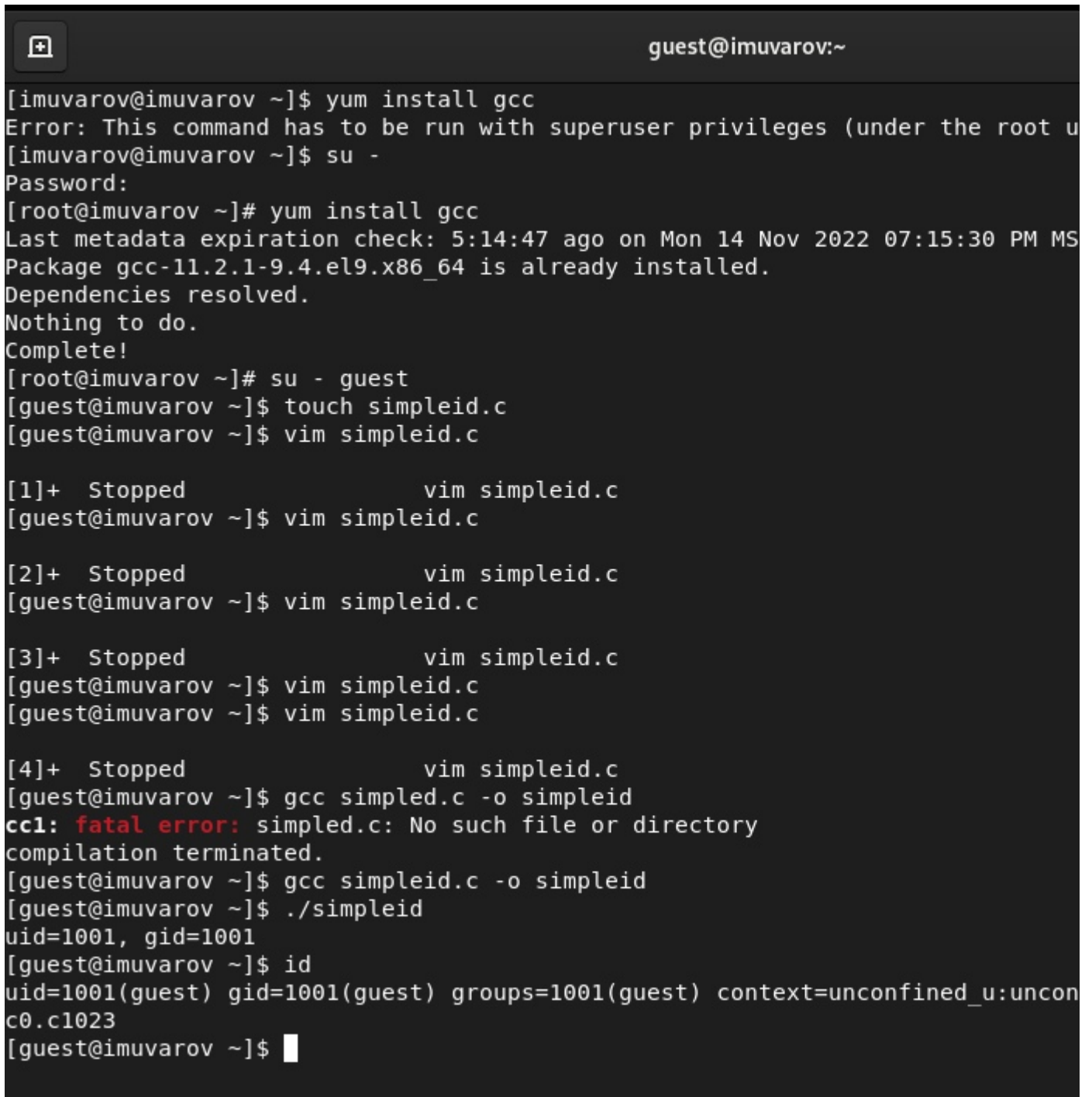
Выполнение лабораторной работы

1. Вошёл в систему от имени пользователя guest и создал программу simpleid.c (рис. 1).



```
#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;
}
~
~
```

2. Скомпилировал программу и убедился, что файл программы создан. Выполнил программу simpleid. Выполнил системную программу id. В отличие от команды id, моя программа не выводит контекст и все группы, в которые пользователь (рис. 2).



```
guest@imuvarov:~  
[imuvarov@imuvarov ~]$ yum install gcc  
Error: This command has to be run with superuser privileges (under the root u  
[imuvarov@imuvarov ~]$ su -  
Password:  
[root@imuvarov ~]# yum install gcc  
Last metadata expiration check: 5:14:47 ago on Mon 14 Nov 2022 07:15:30 PM MS  
Package gcc-11.2.1-9.4.el9.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@imuvarov ~]# su - guest  
[guest@imuvarov ~]$ touch simpleid.c  
[guest@imuvarov ~]$ vim simpleid.c  
  
[1]+  Stopped                  vim simpleid.c  
[guest@imuvarov ~]$ vim simpleid.c  
  
[2]+  Stopped                  vim simpleid.c  
[guest@imuvarov ~]$ vim simpleid.c  
  
[3]+  Stopped                  vim simpleid.c  
[guest@imuvarov ~]$ vim simpleid.c  
[guest@imuvarov ~]$ vim simpleid.c  
  
[4]+  Stopped                  vim simpleid.c  
[guest@imuvarov ~]$ gcc simpleid.c -o simpleid  
cc1: fatal error: simpleid.c: No such file or directory  
compilation terminated.  
[guest@imuvarov ~]$ gcc simpleid.c -o simpleid  
[guest@imuvarov ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@imuvarov ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:uncon  
c0.c1023  
[guest@imuvarov ~]$
```

3. Усложнил программу, добавив вывод действительных идентификаторов (рис. 3).

```

#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;
}
~
~

```

4. Получившуюся программу назвал simpleid2.c. Скомпилировал и запустил simpleid2.c (рис. 4).

```

[guest@imuvarov ~]$ gcc simpleid2.c -o simpleid2
cc1: fatal error: simpleid2.c: No such file or directory
compilation terminated.
[guest@imuvarov ~]$ mv simplified.c simplified2.c
mv: cannot stat 'simplified.c': No such file or directory
[guest@imuvarov ~]$ mv simpleid.c simpleid2.c
[guest@imuvarov ~]$ gcc simpleid2.c -o simpleid2
[guest@imuvarov ~]$ ./simpleid
uid=1001, gid=1001
[guest@imuvarov ~]$ vim simpleid.c

[8]+  Stopped                  vim simpleid.c
[guest@imuvarov ~]$ vim simpleid2.c

[9]+  Stopped                  vim simpleid2.c
[guest@imuvarov ~]$
[guest@imuvarov ~]$ gcc simpleid2.c -o simpleid2
[guest@imuvarov ~]$ ./simpleid
uid=1001, gid=1001
[guest@imuvarov ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@imuvarov ~]$

```

5. От имени суперпользователя выполнил команды `chown root:guest /home/guest/simpleid2` и `chmod u+s /home/guest/simpleid2`. Первая команда меняет владельца файла `simpleid2` на группу `guest`. Вторая команда меняет права доступа к файлу `simpleid2` для пользователя и установленные атрибуты SUID или SGID позволяют запускать файл на выполнение с правами владельца файла или группы соответственно. Выполнил проверку правильности установки новых атрибутов и смены владельца файла `simpleid2`. Запустил `simpleid2` и `id`.

Сравнил результаты (рис. 5).

```
[guest@imuvarov ~]$ su -
Password:
[root@imuvarov ~]# chown root:guest /home/guest/simpleid2
[root@imuvarov ~]# chmod u+s /home/guest/simpleid2
[root@imuvarov ~]# ls -l simpleid2
ls: cannot access 'simpleid2': No such file or directory
[root@imuvarov ~]# ls -l simpleid2
ls: cannot access 'simpleid2': No such file or directory
[root@imuvarov ~]# pwd
/root
[root@imuvarov ~]# cd /home/guest
[root@imuvarov guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26008 Nov 15 01:16 simpleid2
[root@imuvarov guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@imuvarov guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unco
[root@imuvarov guest]#
```

6. Проделал тоже самое относительно SetGID-бита (рис. 6).

```
[guest@imuvarov ~]$ su -
Password:
[root@imuvarov ~]# chown root:guest /home/guest/simpleid2
[root@imuvarov ~]# chmod u+s /home/guest/simpleid2
[root@imuvarov ~]# ls -l simpleid2
ls: cannot access 'simpleid2': No such file or directory
[root@imuvarov ~]# ls -l simpleid2
ls: cannot access 'simpleid2': No such file or directory
[root@imuvarov ~]# pwd
/root
[root@imuvarov ~]# cd /home/guest
[root@imuvarov guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26008 Nov 15 01:16 simpleid2
[root@imuvarov guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@imuvarov guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unco
[root@imuvarov guest]#
```

7. Создал программу readfile.c (рис. 7).

```
#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;
}
```

8. Откомпилировал программу. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог. Проверил, что пользователь guest не может прочитать файл readfile.c. Сменил у программы readfile владельца и установил SetU'D-бит. Проверил, может ли программа readfile прочитать файл readfile.c (рис. 8).


```

did 0(/root);gid 0(/root);groups 0(/root);context unconfined_u:unconfined_t:file
[root@imuvarov guest]# touch readfile.c
[root@imuvarov guest]# vim readfile.c
[root@imuvarov guest]#
[root@imuvarov guest]# vim readfile.c
[root@imuvarov guest]# gcc readfile.c -o readfile
[root@imuvarov guest]# chown root readfile.c
[root@imuvarov guest]# chmod og-rwx readfile.c
[root@imuvarov guest]# exit
logout
[guest@imuvarov ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@imuvarov ~]$ su -
Password:
[root@imuvarov ~]# chmod u+s /home/guest/readfile
[root@imuvarov ~]# ./readfile
-bash: ./readfile: No such file or directory
[root@imuvarov ~]# cd /home/guest
[root@imuvarov guest]# ./readfile
@@N0g000000000000000Pig0@@V@0hyW0!0`*000hyW0V@000g>@!00Cn!0j
0s0nhyW0-0^[00ig0xyW>@hyW0xyW0 00g0p@`yW00@XyW0t~W0~W00~W00~W00~W00~W00~W00~
00g00000&p00@' W00' W00' W0!P0W030000d@@8
ylW000' W00lW00-0^[01
000Rix86_64./readfileSHELL=/bin/bashHISTCONTROL=ignoredup
arrov.localdomainPWD=/home/guestLOGNAME=rootHOME=/rootLANG=en_US.UTF-8LS_COLO
=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;37;
1:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.
01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;
.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31
bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=0
:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.c
;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:
mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tg
;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;3
mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.o
1;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35
lc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;
.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=01;36:*.au=01;36:*.flac
36:*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=01;36:*.ra=01;36:*.
s=01;36:*.spx=01;36:*.xspf=01;36:TERM=xterm-256colorLESSOPEN=||/usr/bin/less
ich_declare=declare -fXDG_DATA_DIRS=/root/.local/share/flatpak/exports/share
are:/usr/local/share:/usr/sharePATH=/root/.local/bin:/root/bin:/usr/local/sb
/usr/binMAIL=/var/spool/mail/rootBASH_FUNC_which%%=( ) { ( alias;
eval ${which_declare} ) | /usr/bin/which --tty-only --read-alias --read-fun
ot "$@"
Segmentation fault (core dumped)
[root@imuvarov guest]#

```

9. Выяснил, установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создал файл file01.txt в директории/tmp со словом test. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» (рис. 9).

```
[root@imuvarov guest]# ls -l | grep tmp
[root@imuvarov guest]# echo "test" > /tmp/file01.txt
[root@imuvarov guest]# ls -l /tmp/file01.txt
-rw-r--r--. 1 root root 5 Nov 15 01:34 /tmp/file01.txt
[root@imuvarov guest]# chmod o+rw /rmp/file01.txt
chmod: cannot access '/rmp/file01.txt': No such file or directory
[root@imuvarov guest]# chmod o+rw /tmp/file01.txt
[root@imuvarov guest]# ls -l /tmp/file01.txt
-rw-r--rw-. 1 root root 5 Nov 15 01:34 /tmp/file01.txt
```

10. От пользователя guest2 попробовал прочитать файл /tmp/file01.txt. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал удалить файл /tmp/file01.tx. Не удалось выполнить операцию. Повысил свои права до суперпользователя и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. Покинул режим суперпользователя. От пользователя guest2 проверил, что атрибута t у директории /tmp нет. Повторил предыдущие шаги. Удалось успешно выполнить каждый шаг. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp (рис. 10).

```
[root@imuvarov guest]# su - guest2
[guest2@imuvarov ~]$ cat /tmp/file01.txt
test
[guest2@imuvarov ~]$ echo "test2" > /tmp/file01.txt
[guest2@imuvarov ~]$ cat /tmp/file01.txt
test2
[guest2@imuvarov ~]$ echo "test3" > /tmp/file01.txt
[guest2@imuvarov ~]$ cat /tmp/file01.txt
test3
[guest2@imuvarov ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@imuvarov ~]$ cd /home/guest
[guest2@imuvarov guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@imuvarov guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@imuvarov guest]$ su -
Password:
[root@imuvarov ~]# chmod -t /tmp
[root@imuvarov ~]# exit
```

Выводы

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.