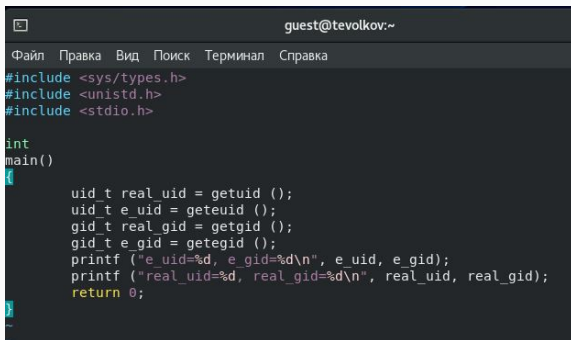


Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Волков Тимофей Евгеньевич НПИбд-01-18

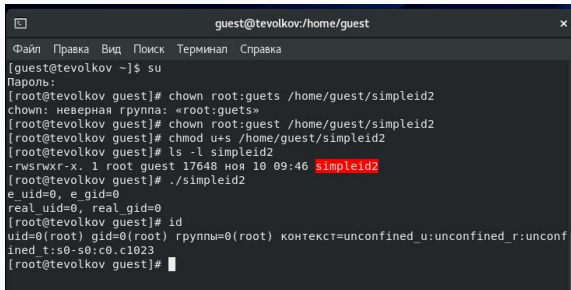
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.



```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
#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;  
}
```

Figure 1: Программа simpleid2.c

Изучение SetUID- SetGID-бита

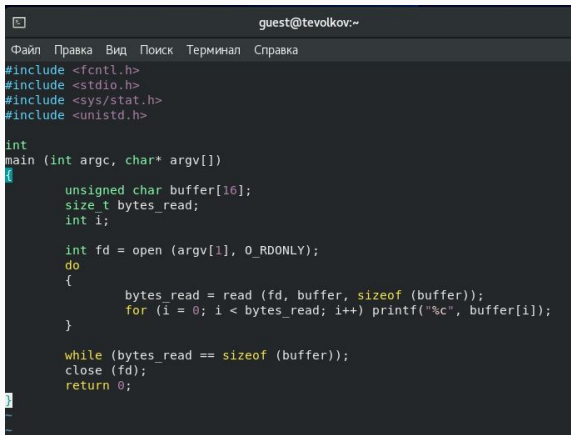


```
guest@tevolkov:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@tevolkov ~]$ su
Пароль:
[root@tevolkov guest]# chown root:guets /home/guest/simpleid2
chown: неверная группа: «root:guets»
[root@tevolkov guest]# chown root:guest /home/guest/simpleid2
[root@tevolkov guest]# chmod u+s /home/guest/simpleid2
[root@tevolkov guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 ноя 10 09:46 simpleid2
[root@tevolkov guest]# ./simpleid2
e_uid=0, e_gid=0
real uid=0, real_gid=0
[root@tevolkov guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tevolkov guest]#
```

Figure 2: Установка SetUID-бита

```
[root@tevolkov guest]# chmod g+s /home/guest/simpleid2
[root@tevolkov guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@tevolkov guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@tevolkov guest]#
```

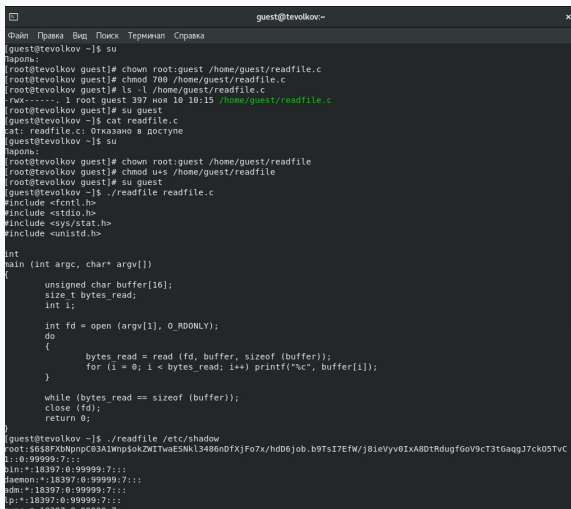
Figure 3: Установка SetGID-бита



```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
#include <fcntl.h>  
#include <stdio.h>  
#include <sys/stat.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;  
}
```

Figure 4: Программа readfile.c

Изучение SetUID- SetGID-бита



```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@tevolkov ~]$ su  
Пароль:  
[root@tevolkov guest]# chown root:guest /home/guest/readfile.c  
[root@tevolkov guest]# chmod 700 /home/guest/readfile.c  
[root@tevolkov guest]# ls -l /home/guest/readfile.c  
-rwx-----. 1 root guest 397 ноя 10 10:15 /home/guest/readfile.c  
[root@tevolkov guest]# su guest  
[guest@tevolkov ~]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@tevolkov ~]$ su  
Пароль:  
[root@tevolkov guest]# chown root:guest /home/guest/readfile  
[root@tevolkov guest]# chmod u+s /home/guest/readfile  
[root@tevolkov guest]# su guest  
[guest@tevolkov ~]$ ./readfile readfile.c  
#include <fcntl.h>  
#include <stdio.h>  
#include <sys/stat.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@tevolkov ~]$ ./readfile /etc/shadow  
root:$6$8FXbnpnc03A1Wnp$okZWITwaESNk13486nDfXjFo7x/hdD6job.b9TsI7EfW/j8ieVvY0IxAB0tRdugfGoV9cT3tGaagJ7ck05Tvc  
1::0:99999:7:::  
bin:*.18397:0:99999:7:::  
daemon:*.18397:0:99999:7:::  
adm:*.18397:0:99999:7:::  
lp:*.18397:0:99999:7:::  
nrc:*.18397:0:99999:7:::
```

Figure 5: Проверка работы программы readfile

Исследование Sticky-бита

```
guest2@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
guest@tevolkov ~]$ ls -l |grep tmp  
guest@tevolkov ~]$ ls -l | grep tmp  
guest@tevolkov ~]$ ls -l / | grep tmp  
drwxrwxrwt. 14 root root 4096 ноя 10 10:20 tmp  
guest@tevolkov ~]$ echo "test" > /tmp/file01.txt  
guest@tevolkov ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 ноя 10 10:29 /tmp/file01.txt  
guest@tevolkov ~]$ chmod o+rw /tmp/file01.txt  
guest@tevolkov ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 ноя 10 10:29 /tmp/file01.txt  
guest@tevolkov ~]$ su guest2  
Пароль:  
guest2@tevolkov guest]$ exit  
exit  
guest@tevolkov ~]$ su - guest2  
Пароль:  
guest2@tevolkov ~]$ cat /tmp/file01.txt  
test  
guest2@tevolkov ~]$ echo "test2" > /tmp/file01.txt  
guest2@tevolkov ~]$ cat /tmp/file01.txt  
test2  
guest2@tevolkov ~]$ echo "test2" /tmp/file01.txt  
test2 /tmp/file01.txt  
guest2@tevolkov ~]$ cat /tmp/file01.txt  
test2  
guest2@tevolkov ~]$ echo "test3" > /tmp/file01.txt  
guest2@tevolkov ~]$ cat /tmp/file01.txt  
test3  
guest2@tevolkov ~]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': операция не позволена  
guest2@tevolkov ~]$ su -  
Пароль:  
root@tevolkov ~]# chmod -t /tmp  
root@tevolkov ~]# exit  
Выход  
guest2@tevolkov ~]$ ls -l / | grep tmp  
drwxrwxrwx. 14 root root 4096 ноя 10 10:35 tmp  
guest2@tevolkov ~]$ echo "test2" > /tmp/file01.txt  
guest2@tevolkov ~]$ cat /tmp/file01.txt  
test2  
guest2@tevolkov ~]$ rm /tmp/file01.txt  
guest2@tevolkov ~]$ su -  
Пароль:  
root@tevolkov ~]# chmod +t /tmp  
root@tevolkov ~]# exit  
Выход  
guest2@tevolkov ~]$
```