

Лабораторная работа 5

Юдин Герман Станиславович, НФИбд-01-19

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Юдин Герман Станиславович

Группа: НФИбд-01-19

МОСКВА

2022 г.

Цель работы

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. uid, gid (1)

1. uid, gid (1)

```
[guest@gsyudin Work]$ cat 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;
}
[guest@gsyudin Work]$ gcc simpleid.c
[guest@gsyudin Work]$ ls
a.out  readfile.c  simpleid2.c  simpleid.c
[guest@gsyudin Work]$ ./a.out
uid=1001, gid=1001
[guest@gsyudin Work]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),976(vboxsf) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 1: simpleid

1. uid, gid (2)

1. uid, gid (2)

```
[guest@gsyudin Work]$ cat simpleid2.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;
}
[guest@gsyudin Work]$ gcc simpleid2.c
[guest@gsyudin Work]$ ls
a.out  readfile.c  simpleid2.c  simpleid.c
[guest@gsyudin Work]$ ./a.out
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Figure 2: simpleid2

2. s bit

2. s bit

```
[guest@gsyudin Work]$ ls -l
total 68
-rwxrwxr-x. 1 guest guest 26008 Sep 27 21:40 a.out
-rwxrwx---. 1 guest guest  479 Sep 27 21:37 readfile.c
-rwsrwxr-x. 1 root  guest 26008 Sep 27 21:41 simpleid2
-rwxrwx---. 1 guest guest  345 Sep 27 21:37 simpleid2.c
-rwxrwx---. 1 guest guest  203 Sep 27 21:37 simpleid.c

[guest@gsyudin Work]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@gsyudin Work]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),976(vboxsf) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

3. Чтение файлов с правами администратора

3. Чтение файлов с правами администратора

```
[root@gsyudin ~]# chown root:guest /home/guest/Work/readfile
[root@gsyudin ~]# chmod u+s /home/guest/Work/readfile

[guest@gsyudin Work]$ ./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;
}
```

4. Каталог tmp

4. Каталог tmp

Данный атрибут не даёт менять файл, в том числе нельзя удалять файл.

```
[guest@gsyudin Work]$ ls -l / | grep tmp  
drwxrwxrwt. 17 root root 4096 Sep 27 21:54 tmp  
[guest@gsyudin Work]$ echo "test" > /tmp/file01.txt
```

5. Файл file.txt

5. Файл file.txt

```
[guest2@gsyudin ~]$ cat /tmp/file01.txt
test
[guest2@gsyudin ~]$ echo "test2" > /tmp/file01.txt
[guest2@gsyudin ~]$ cat /tmp/file01.txt
test2
[guest2@gsyudin ~]$ echo "test3" >> /tmp/file01.txt
[guest2@gsyudin ~]$ cat /tmp/file01.txt
test2
test3
[guest2@gsyudin ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Вывод

Вывод

Выполнив данную лабораторную работу, я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получил практические навыки работы в консоли с дополнительными атрибутами, рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

