

Информационная безопасность

Лабораторная работа №5

Матюшкин Д. В.

23 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Матюшкин Денис Владимирович
- студент 4-го курса
- группа НПИбд-02-21
- Российский университет дружбы народов
- 1032212279@pfur.ru
- <https://stifell.github.io/ru/>



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

Создание программы

1. Создайте программу simpleid.c

```
[guest@dvmatyushkin ~]$ touch simpleid.c
[guest@dvmatyushkin ~]$ nano simpleid.c
```

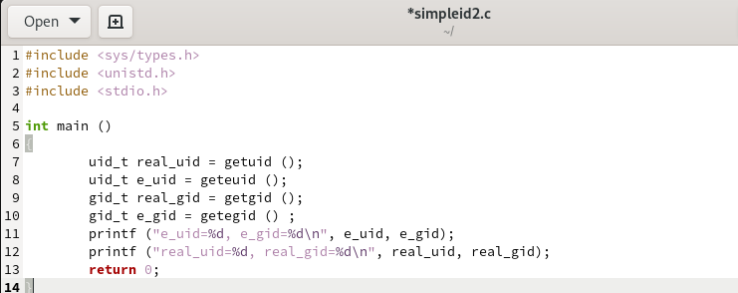


```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int main ()
6 {
7     uid_t uid = geteuid ();
8     gid_t gid = getegid ();
9     printf ("uid=%d, gid=%d\n", uid, gid);
10    return 0;
11 }
```

Рис. 1: simpleid.c

2. Скомпилируйте программу

```
[guest@dvmatyushkin ~]$ ./simpleid
uid=1001, gid=1001
[guest@dvmatyushkin ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
[guest@dvmatyushkin ~]$ touch simpleid2.c
[guest@dvmatyushkin ~]$
```

```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int main ()
6 {
7     uid_t real_uid = getuid ();
8     uid_t e_uid = geteuid ();
9     gid_t real_gid = getgid ();
10    gid_t e_gid = getegid ();
11    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
12    printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
13    return 0;
14 }
```

Рис. 2: Выполнение программы simpleid

3. Скомпилируйте и запустите simpleid2.c

```
[guest@dvmatyushkin ~]$ gcc simpleid2.c -o simpleid2  
[guest@dvmatyushkin ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001
```

Рис. 3: Выполнение программы simpleid2

4. От имени суперпользователя выполните команды

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

Рис. 4: Выполнение команд

5. Выполните проверку правильности установки новых атрибутов

```
[guest@dvmatyushkin ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 17720 Oct  3 15:58 simpleid2
[guest@dvmatyushkin ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@dvmatyushkin ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
[guest@dvmatyushkin ~]$
```

Рис. 5: Проверка атрибутов и запуск программы

6.1. Проделайте тоже самое относительно SetGID-бита

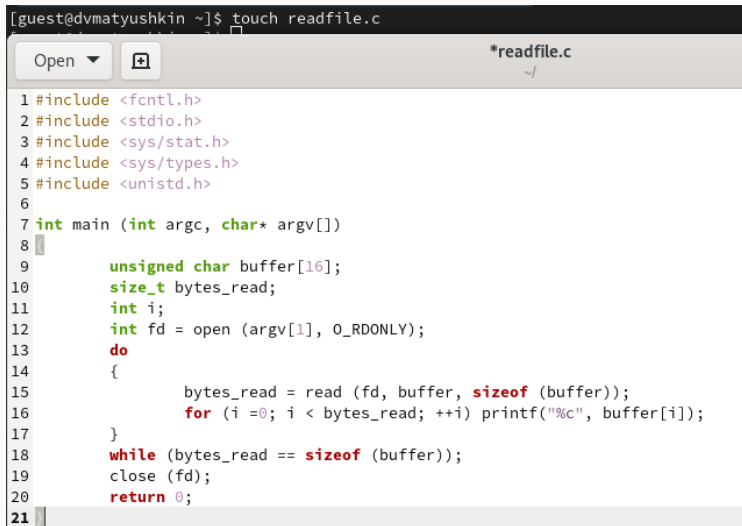
```
[root@dvmatyushkin guest]# chmod g+s /home/guest/simpleid2  
[root@dvmatyushkin guest]#
```

Рис. 6: Установка SetGID-бита

```
[guest@dvmatyushkin ~]$ ls -l simpleid2
-rwsr-sr-x. 1 root guest 17720 Oct  3 15:58 simpleid2
[guest@dvmatyushkin ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@dvmatyushkin ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_
```

Рис. 7: Проверка атрибутов и запуск программы

7. Создайте программу readfile.c



```
[guest@dvmatyushkin ~]$ touch readfile.c

Open [icon] *readfile.c ~/

1 #include <fcntl.h>
2 #include <stdio.h>
3 #include <sys/stat.h>
4 #include <sys/types.h>
5 #include <unistd.h>
6
7 int main (int argc, char* argv[])
8 {
9     unsigned char buffer[16];
10    size_t bytes_read;
11    int i;
12    int fd = open (argv[1], O_RDONLY);
13    do
14    {
15        bytes_read = read (fd, buffer, sizeof (buffer));
16        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
17    }
18    while (bytes_read == sizeof (buffer));
19    close (fd);
20    return 0;
21 }
```

Рис. 8: readfile.c

8. Смените владельца и права у файла readfile.c

```
[root@dvmatyushkin guest]# chown guest2:guest /home/guest/readfile  
[root@dvmatyushkin guest]# ^C  
[root@dvmatyushkin guest]# chmod u+s /home/guest/readfile
```

Рис. 9: Смена владельца и установка SetUID

9. Проверьте, что пользователь `guest` не может прочитать файл `readfile.c`

[illegible]

10. Выполнение команд

- Смените у программы `readfile` владельца и установите SetUID-бит (рис. 9).
- Проверьте, может ли программа `readfile` прочитать файл `readfile.c` (рис. 10).
- Проверьте, может ли программа `readfile` прочитать файл `/etc/shadow` (рис. 10).

Исследование Sticky-бита

- Выясните, установлен ли атрибут Sticky на директории /tmp (рис. 11).
- От имени пользователя guest создайте файл file01.txt (рис. 11).
- Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» (рис. 11).

1.2. Скриншот

```
[guest@dvmatyushkin ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct  3 16:11 tmp
[guest@dvmatyushkin ~]$ echo "test" > /tmp/file01.txt
[guest@dvmatyushkin ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  3 16:13 /tmp/file01.txt
[guest@dvmatyushkin ~]$ chmod o+rw /tmp/file01.txt
[guest@dvmatyushkin ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  3 16:13 /tmp/file01.txt
[guest@dvmatyushkin ~]$
```

Рис. 11: Работа в директории /tmp

2.1. Работа с файлом file01.txt

- От пользователя guest2 попробуйте прочитать файл /tmp/file01.txt (рис. 12).
- От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 (рис. 12).
- Проверьте содержимое файла (рис. 12).
- От пользователя guest2 попробуйте записать в файл
- Проверьте содержимое файла
- От пользователя guest2 попробуйте удалить файл /tmp/file01.txt

2.2. Скриншот

```
[guest2@dvmatyushkin guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dvmatyushkin guest]$ cat /tmp/file01.txt
test
[guest2@dvmatyushkin guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dvmatyushkin guest]$ cat /tmp/file01.txt
test
[guest2@dvmatyushkin guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
```

Рис. 12: Работа с файлом file01.txt

3. Повысьте свои права до суперпользователя и выполните после этого команду, снимающую атрибут t (Sticky-бит)

```
[guest2@dvmatyushkin guest]$ su -  
Password:  
[root@dvmatyushkin ~]# chmod -t /tmp  
[root@dvmatyushkin ~]# exit  
logout  
[guest2@dvmatyushkin guest]$ ls -l / | grep tmp  
drwxrwxrwx. 17 root root 4096 Oct  3 16:16 tmp  
[guest2@dvmatyushkin guest]$
```

Рис. 13: Снятие Sticky-бит с директории /tmp

- От пользователя guest2 проверьте, что атрибута t у директории /tmp нет (рис. 13).
- Повторите предыдущие шаги. Теперь можем все то же самое, но еще и удалять файл (рис. 14).

4.2. Скриншот

```
[guest2@dvmatyushkin tmp]$ cat /tmp/file01.txt
test
[guest2@dvmatyushkin tmp]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dvmatyushkin tmp]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dvmatyushkin tmp]$ cat /tmp/file01.txt
test
[guest2@dvmatyushkin tmp]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dvmatyushkin tmp]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@dvmatyushkin tmp]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
```

Рис. 14: Повторение действий с file01.txt

5. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp

```
[guest2@dvmatyushkin tmp]$ su -  
Password:  
[root@dvmatyushkin ~]# chmod +t /tmp  
[root@dvmatyushkin ~]# exit  
logout
```

Рис. 15: Возвращение Sticky-бит в директорию /tmp

Выводы

- В ходе данной лабораторной работы мы изучили механизм изменения идентификаторов, применение SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.