

Лабораторная работа №5

Дискреционное разграничение прав в Linux.

Исследование влияния дополнительных атрибутов.

Монастырская Кристина Владимировна НПИбд-02-19¹

2022, 19 March, Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

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.

Создала программу simpleid.c

Создала программу simpleid.c



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

Рис. 1: Код программы simpleid.c

Компилирование и запуск программы

```
[guest@kvmonastyrskaya ~]$ gcc simpleid.c -o simpleid
```

Рис. 2: Компилирование программы simpleid

Усложнение программы

```
[guest@kvmonastyrskaya ~]$ ./simpleid  
uid=1001, gid=1001
```

Рис. 3: Выполнение программы simpleid

Работа второй программы

```
[guest@kvmonastyrskaya ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001
```

Рис. 4: Выполнение simpleid2

Смена владельца и группы файла
simpleid2 и его прав доступа

Смена владельца и группы файла simpleid2 и его прав доступа

```
[root@kvmonastyrskaya ~]# chown root:guest /home/guest/simpleid2  
[root@kvmonastyrskaya ~]# chmod u+s /home/guest/simpleid2  
[root@kvmonastyrskaya ~]#
```

Рис. 5: Смена владельца и атрибутов

Правильность установки новых атрибутов

Правильность установки новых атрибутов

```
[guest@kvmonastyrskaya ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kvmonastyrskaya ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@kvmonastyrskaya ~]$
```

Рис. 6: Проверка установленных атрибутов

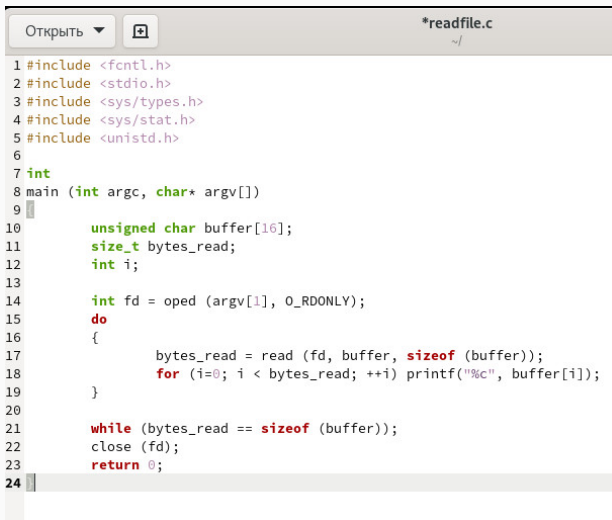
Проделали тоже самое относительно
SetGID-бита

Проделили тоже самое относительно SetGID-бита

```
[guest@kvmonastyrskaya ~]$ su -
Пароль:
[root@kvmonastyrskaya ~]# ch^C
[root@kvmonastyrskaya ~]# chown root:guest /home/guest/simpleid2
[root@kvmonastyrskaya ~]# chmod g+s /home/guest/simpleid2
[root@kvmonastyrskaya ~]# su - guest
[guest@kvmonastyrskaya ~]$ ls -l simpleid2
-rwxrwsr-x. 1 root guest 26048 дек 18 14:37 simpleid2
[guest@kvmonastyrskaya ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kvmonastyrskaya ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@kvmonastyrskaya ~]$
```

Рис. 7: SetGID-бит

Программа readfile.c



```
1 #include <fcntl.h>
2 #include <stdio.h>
3 #include <sys/types.h>
4 #include <sys/stat.h>
5 #include <unistd.h>
6
7 int
8 main (int argc, char* argv[])
9 {
10     unsigned char buffer[16];
11     size_t bytes_read;
12     int i;
13
14     int fd = open (argv[1], O_RDONLY);
15     do
16     {
17         bytes_read = read (fd, buffer, sizeof (buffer));
18         for (i=0; i < bytes_read; ++i) printf("%c", buffer[i]);
19     }
20
21     while (bytes_read == sizeof (buffer));
22     close (fd);
23     return 0;
24 }
```

Рис. 8: Программа readfile.c

Компиляция readfile.c

```
[guest@kvmonastyrskaya ~]$ gcc readfile.c -o readfile
```

Рис. 9: Компилирование readfile

Смена владельца файла readfile.c

Смена владельца файла readfile.c

```
[root@kvmonastyrskaya ~]# cd /home/guest
[root@kvmonastyrskaya guest]# chown root readfile.c
[root@kvmonastyrskaya guest]# ls -l
итого 92
drwxr-xr-x. 2 guest guest    19 дек 15 19:44  dir1
-rwxr-xr-x. 1 guest guest 25992 дек 18 15:02  readfile
-rw-r--r--. 1 root  guest   421 дек 18 15:02  readfile.c
-rwxrwxr-x. 1 guest guest 25944 дек 18 14:34  simpleid
-rwxrwsr-x. 1 root  guest 26048 дек 18 14:37  simpleid2
-rw-rw-r--. 1 guest guest   310 дек 18 14:38  simpleid.c
```

Рис. 10: Смена владельца readfile.c

Изменение прав

Изменение прав

```
[root@kvmonastyrskaya guest]# chmod 000 readfile.c
[root@kvmonastyrskaya guest]# ls -l
итого 92
drwxr-xr-x. 2 guest guest    19 дек 15 19:44  dir1
-rwxr-xr-x. 1 guest guest 25992 дек 18 15:02  readfile
-----, 1 root  guest    421 дек 18 15:02  readfile.c
-rwxrwxr-x. 1 guest guest 25944 дек 18 14:34  simpleid
-rwxrwsr-x. 1 root  guest 26048 дек 18 14:37  simpleid2
-rw-rw-r--. 1 guest guest   310 дек 18 14:38  simpleid.c
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Видео
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Документы
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Загрузки
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Изображения
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Музыка
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Общедоступные
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  'Рабочий стол'
drwxr-xr-x. 2 guest guest     6 дек 15 16:28  Шаблоны
[root@kvmonastyrskaya guest]# chmod u+r readfile.c
[root@kvmonastyrskaya guest]# ls -l
итого 92
drwxr-xr-x. 2 guest guest    19 дек 15 19:44  dir1
-rwxr-xr-x. 1 guest guest 25992 дек 18 15:02  readfile
-r-----, 1 root  guest    421 дек 18 15:02  readfile.c
```

Рис. 11: Изменение атрибутов readfile.c

Проверка

```
[guest@kvmonastyrskaya ~]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@kvmonastyrskaya ~]$
```

Рис. 12: Проверка чтения файла

Смена владельца и установка SetUID-бит

Смена владельца и установка SetUID-бит

```
[root@kvmonastyrskaya ~]# cd /home/guest
[root@kvmonastyrskaya guest]# chown root readfile
[root@kvmonastyrskaya guest]# ls -l
итого 92
drwxr-xr-x. 2 guest guest    19 дек 15 19:44 dir1
-rwxr-xr-x. 1 root  guest 25992 дек 18 15:02 readfile
-r------. 1 root  guest   421 дек 18 15:02 readfile.c
-rwxrwxr-x. 1 guest guest 25944 дек 18 14:34 simpleid
-rwxrwsr-x. 1 root  guest 26048 дек 18 14:37 simpleid2
-rw-rw-r--. 1 guest guest   310 дек 18 14:38 simpleid.c
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Видео
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Документы
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Загрузки
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Изображения
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Музыка
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Общедоступные
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 'Рабочий стол'
drwxr-xr-x. 2 guest guest     6 дек 15 16:28 Шаблоны
[root@kvmonastyrskaya guest]# chmod u+s readfile
[root@kvmonastyrskaya guest]# ls -l
итого 92
drwxr-xr-x. 2 guest guest    19 дек 15 19:44 dir1
-rwsr-xr-x. 1 root  guest 25992 дек 18 15:02 readfile
-r------. 1 root  guest   421 дек 18 15:02 readfile.c
```

Рис. 13: Смена владельца и установка SetU'D-бита

Выполнение программы reafire

Выполнение программы readfile

```
[guest@kvmonastyrskaya ~]$ ./readfile /etc/shadow
root:$6$IjTYgIcu4bHIm.W$Zp0ARLCVMHNP9eJhHLInq0H08K2j1M00cNUZVN1y1YQs2gSifJ7SqoF
jy9J0g6G.h3yLkBy/i.rvG0FnFI7090::0:99999:7:::
bin:!:19121:0:99999:7:::
daemon:!:19121:0:99999:7:::
adm:!:19121:0:99999:7:::
lp:!:19121:0:99999:7:::
sync:!:19121:0:99999:7:::
shutdown:!:19121:0:99999:7:::
halt:!:19121:0:99999:7:::
mail:!:19121:0:99999:7:::
operator:!:19121:0:99999:7:::
games:!:19121:0:99999:7:::
ftp:!:19121:0:99999:7:::
nobody:!:19121:0:99999:7:::
systemd-coredump:!!!:19341:::
dbus:!!!:19341:::
polkitd:!!!:19341:::
```

Рис. 14: Чтение файла /etc/shadow программой из readfile

Чтение файла /etc/shadow

Чтение файла /etc/shadow

```
[guest@kvmonastyrskaya ~]$ ./readfile /etc/shadow
root:$6$IjTYgIcu4bHIm.W$Zp0ARLCVMHNP9eJhHLInq0H08K2j1M00cNUZVN1y1YQs2gSifJ7SqoF
jy9J0g6G.h3yLkBy/i.rvG0FnFI7090::0:99999:7:::
bin:!:19121:0:99999:7:::
daemon:!:19121:0:99999:7:::
adm:!:19121:0:99999:7:::
lp:!:19121:0:99999:7:::
sync:!:19121:0:99999:7:::
shutdown:!:19121:0:99999:7:::
halt:!:19121:0:99999:7:::
mail:!:19121:0:99999:7:::
operator:!:19121:0:99999:7:::
games:!:19121:0:99999:7:::
ftp:!:19121:0:99999:7:::
nobody:!:19121:0:99999:7:::
systemd-coredump:!!!:19341:::
dbus:!!!:19341:::
polkitd:!!!:19341:::
```

Рис. 15: Чтение файла /etc/shadow программой из readfile

Наличие атрибута Sticky на
директории /tmp

Наличие атрибута Sticky на директории /tmp

```
[guest@kvmonastyrskaya ~]$ ls -l / |grep tmp
drwxrwxrwt. 22 root root 4096 дек 18 15:10 tmp
[guest@kvmonastyrskaya ~]$
```

Рис. 16: Атрибут Sticky на директории /tmp

Создали файл file01.txt в директории
/tmp со словом test

Создали файл file01.txt в директории /tmp со словом test

```
[guest@kvmonastyrskaya ~]$ echo "test" > /tmp/file01.txt
```

Рис. 17: Создание файла file01.txt в директории /tmp

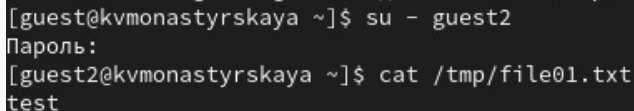
Чтение и запись для категории
пользователей «все остальные»

```
[guest@kvmonastyrskaya ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 дек 18 15:12 /tmp/file01.txt
[guest@kvmonastyrskaya ~]$ chmod o+rw /tmp/file01.txt
[guest@kvmonastyrskaya ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 дек 18 15:12 /tmp/file01.txt
[guest@kvmonastyrskaya ~]$
```

Рис. 18: Чтение и запись для категории пользователей «все остальные»

От пользователя guest2 прочитали
файл /tmp/file01.txt

От пользователя guest2 прочитали файл /tmp/file01.txt

A terminal window with a black background and white text. The first line shows a user switch from 'guest' to 'guest2' using the 'su' command. The second line shows the password prompt. The third line shows the execution of the 'cat' command to read the contents of '/tmp/file01.txt', which outputs the word 'test'.

```
[guest@kvmonastyrskaya ~]$ su - guest2
Пароль:
[guest2@kvmonastyrskaya ~]$ cat /tmp/file01.txt
test
```

Рис. 19: Чтение файла /tmp/file01.txt

От пользователя guest2 дозаписали
файл /tmp/file01.txt

От пользователя guest2 дозаписали файл /tmp/file01.txt

```
[guest2@kvmonastyrskaya ~]$ echo "test2" > /tmp/file01.txt  
-bash: /tmp/file01.txt: Отказано в доступе  
[guest2@kvmonastyrskaya ~]$
```

Рис. 20: Дозапись файла /tmp/file01.txt

От пользователя guest2 перезапись
файла /tmp/file01.txt

От пользователя guest2 перезапись файла /tmp/file01.txt

```
[guest2@kvmonastyrskaya ~]$ echo "test3" > /tmp/file01.txt  
-bash: /tmp/file01.txt: Отказано в доступе  
[guest2@kvmonastyrskaya ~]$
```

Рис. 21: Перезапись файла /tmp/file01.txt

Попытка удалить файл /tmp/file01.txt

Попытка удалить файл /tmp/file01.txt

```
[guest2@kvmonastyrskaya ~]$ rm /tmp/file01.txt  
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@kvmonastyrskaya ~]$
```

Рис. 22: Попытка удаления файла /tmp/file01.txt

От пользователя guest2 проверили,
что атрибута t у директории /tmp нет

От пользователя guest2 проверили, что атрибута t у директории /tmp нет

Проверка атрибутов]](.. /images/30.jpg){ #fig:029 width=80% height=80% }

Повторили предыдущие шаги

Повторили предыдущие шаги

```
[guest2@kvmonastyrskaya ~]$ su -  
Пароль:  
[root@kvmonastyrskaya ~]# chmod +t /tmp  
[root@kvmonastyrskaya ~]# exit  
выход  
[guest2@kvmonastyrskaya ~]$
```

Рис. 23: Проверка атрибутов

Вывод

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.