

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Монастырская Кристина Владимировна

Содержание

Цель работы	4
Выполнение лабораторной работы	5
Выводы	15
Список литературы	16

Список иллюстраций

1	Код программы simpleid.c	5
2	Компилирование программы simpleid	5
3	Выполнение программы simpleid	6
4	Выполнение id	6
5	Код программы simpleid2.c	6
6	Смена владельца и атрибутов	7
7	Проверка установки новых атрибутов	7
8	Код программы simpleid.c	7
9	SetGID-бит	7
10	Программа readfile.c	8
11	Компилирование readfile	8
12	Смена владельца readfile.c	9
13	Изменение атрибутов readfile.c	9
14	Проверка чтения файла	10
15	Смена владельца и установка SetU'D-бита	10
16	Чтение файла readfile.c программой readfile	11
17	Чтение файла /etc/shadow программой из readfile	11
18	Атрибут Sticky на директории /tmp	12
19	Создание файла file01.txt в директории /tmp	12
20	Чтение и запись для категории пользователей «все остальные» . .	12
21	Чтение файла /tmp/file01.txt	12
22	Дозапись файла /tmp/file01.txt	13
23	Перезапись файла /tmp/file01.txt	13
24	Проверка содержимого файла /tmp/file01.txt	13
25	Попытка удаления файла /tmp/file01.txt	13
26	Проверка атрибутов	14

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 [1].

Выполнение лабораторной работы

1. Вошла в систему от имени пользователя guest.
2. Создала программу simpleid.c (рис. 1).



```
*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

3. Скомпилировала программу и убедилась, что файл программы создан.(рис. 2)



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

Рис. 2: Компилирование программы simpleid

4. Выполнила программу simpleid (рис. 3).

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

Рис. 3: Выполнение программы simpleid

5. Выполнила системную программу id и сравнила полученный результат с данными предыдущего пункта задания.(рис. 4)

```
[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. 4: Выполнение id

6. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c(рис. 5)



```
*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. 5: Код программы simpleid2.c

7. Скомпилируйте и запустите simpleid2.c:(рис. 6)(рис. 7)

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

8. От имени суперпользователя выполнила команды(рис. 8):

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

Рис. 6: Смена владельца и атрибутов

9. Выполнила проверку правильности установки новых атрибутов и сменила владельца файла simpleid2:(рис. 2)

```
[guest@kvmonastyrskaya ~]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 26048 дек 18 14:37 simpleid2
```

Рис. 7: Проверка установки новых атрибутов

10. Запустила simpleid2 и id(рис. 10)

```
[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. 8: Код программы simpleid.c

11. Проделала тоже самое относительно SetGID-бита.(рис. 11)

```
[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. 9: SetGID-бит

12. Создала программу readfile.c(рис. 12):

Рис. 10: Программа readfile.c

13. Откомпилировала её.(рис. 13)

Рис. 11: Компилирование readfile

14. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.(рис. 14)(рис. 15)


```

[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. 12: Смена владельца readfile.c

```

[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. 13: Изменение атрибутов readfile.c

15. Проверила, что пользователь guest не может прочитать файл readfile.c.(рис. 16)

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

Рис. 14: Проверка чтения файла

16. Сменила у программы readfile владельца и установила SetU'D-бит(рис. 17)

```
[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. 15: Смена владельца и установка SetU'D-бита

17. Проверила, может ли программа readfile прочитать файл readfile.c(рис. 18)

```

[root@kvmonastyrskaya guest]# su - guest
[guest@kvmonastyrskaya ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/types.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@kvmonastyrskaya ~]$

```

Рис. 16: Чтение файла readfile.c программой readfile

18. Проверила, может ли программа readfile прочитать файл /etc/shadow(рис. 19)

```

[guest@kvmonastyrskaya ~]$ ./readfile /etc/shadow
root:$6$IjTYgIcu4bHIm.W$Zp0ARLCVMHNP9eJhHLInq0H08K2jLM00cNUZVN1y1YQs2gSifJ7SgoF
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. 17: Чтение файла /etc/shadow программой из readfile

19. Выяснила, установлен ли атрибут Sticky на директории /tmp (рис. 20)

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

Рис. 18: Атрибут Sticky на директории /tmp

22. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test: echo "test" > /tmp/file01.txt(рис. 21)

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

Рис. 19: Создание файла file01.txt в директории /tmp

23. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные»(рис. 22): ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt

```
[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. 20: Чтение и запись для категории пользователей «все остальные»

24. От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt(рис. 23):

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

Рис. 21: Чтение файла /tmp/file01.txt

25. От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” > /tmp/file01.txt(рис. 24)

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

Рис. 22: Дозапись файла /tmp/file01.txt

26. От пользователя guest2 попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt(рис. 25)

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

Рис. 23: Перезапись файла /tmp/file01.txt

27. Проверила содержимое файла(рис. 26)

```
[guest2@kvmonastyrskaya ~]$ cat /tmp/file01.txt
test
```

Рис. 24: Проверка содержимого файла /tmp/file01.txt

28. От пользователя guest2 попробовала удалить файл /tmp/file01.txt(рис. 27)

```
[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. 25: Попытка удаления файла /tmp/file01.txt

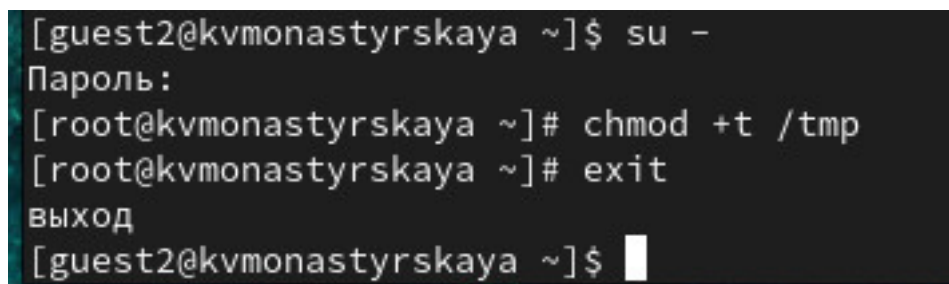
29. Повысила свои права до суперпользователя следующей командой(рис. 28)
su - и выполнила после этого команду, снимающую атрибут t (Sticky-бит)
сдиректории /tmp: chmod -t /tmp

30. Повторила предыдущие шаги(рис. 29)

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

32. Теперь можем удалять файлы находящиеся в каталоге tmp.

33. Повысила свои права до суперпользователя и вернула атрибут t на директо-
рию /tmp(рис. 30): su - chmod +t /tmp exit



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

Рис. 26: Проверка атрибутов

Выводы

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

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.