

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

Захарова Софья Михайловна

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.

За-
да-
ние

Лабораторная

ра-
бота

под-

ра-

зу-

ме-

вает

ра-

боту

с

вир-

ту-

аль-

ной

ма-

ши-

ной

VirtualBox,

опе-

ра-

ци-

он-

ной

си-

сте-

мой

Linux,

дис-

три-

бу-

ти-

вом

Centos

и за-

креп-

ле-

ние

тео-

ре-

ти-

че-

ских

ос-

нов

по-

лу₂

че-

ния

прак-

ти-

че-

ских

на-

вы-

Выполнение лабораторной работы

1. Вошла в систему от имени пользователя guest. (рис.1).



```
[guest@smzakharova1 ~]$
```

Рис. 1: Рис.1. Вход в систему.

2. Создала программу simpleid.c. (рис.2).



```
guest@smzakharova1:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
GNU nano 2.3.1  Файл: 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;  
}
```

Рис. 2: Рис.2. Создание программы.

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



```
[guest@smzakharova1 ~]$ nano simpleid.c  
[guest@smzakharova1 ~]$ gcc simpleid.c -o simpleid  
[guest@smzakharova1 ~]$
```

Рис. 3: Рис.3. Компиляция файла.

4. Выполнила программу simpleid: ./simpleid (рис.4):

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

Рис. 4: Рис.4. Выполнение программы.

5. Выполнила системную программу `id` и сравнила полученный результат с данными предыдущего пункта задания: программа работает верно, результаты совпадают. (рис.5):

```
[guest@smzakharoval ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0-c0:c1023
[guest@smzakharoval ~]$
```

Рис. 5: Рис.5. Выполнение программы и сравнение с предыдущей.

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

```
guest@smzakharoval~
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.3.1  Файл: simpleid.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;
}
```

Рис. 6: Рис.6. Усложнение программы.

7. Скомпилировала и запустила `simpleid2.c` (рис.7).

8. От имени суперпользователя выполнила команды: `chown root:guest /home/guest/simpleid2` `chmod u+s /home/guest/simpleid2` С помощью этих команд файлу `simpleid2` изменила владельца и группу на `root` и `guest` соответственно, а также установила на файл SetUID-бит. (рис. 8).

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

Рис. 7: Рис.7. Компиляция и запуск второй программы.

```
[guest@smzakharoval ~]$ su
Пароль:
[root@smzakharoval guest]#
[root@smzakharoval guest]# chown root:guest /home/guest/simpleid2
[root@smzakharoval guest]# chmod u+s /home/guest/simpleid2
[root@smzakharoval guest]# █
```

Рис. 8: Рис.8. Выполнение команд.

9. Временно повысила свои права с помощью команды su (рис. 9).

```
[guest@smzakharoval ~]$ su
Пароль:
```

Рис. 9: Рис.9. Повышение прав.

10. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls -l simpleid2 (рис. 10).

11. Запустила simpleid2 и id. Результаты совпадают. (рис.11)

12. Проделала тоже самое относительно SetGID-бита (рис.12).

13. Создала программу readfile.c (рис.13).

14. Откомпилировала её (рис.14).

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

```
[root@smzakharoval ~]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8656 ноя 12 16:16 simpleid2
[root@smzakharoval ~]#
```

Рис. 10: Рис.10. Проверка.

```
[root@smzakharoval ~]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@smzakharoval ~]# id
uid=0(root) gid=0(root) rpytty=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@smzakharoval ~]#
```

Рис. 11: Рис.11. Запуск команд.

```
[root@smzakharoval ~]# chown root:guest /home/guest/simpleid2
[root@smzakharoval ~]# chmod u+s /home/guest/simpleid2
[root@smzakharoval ~]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8656 ноя 12 16:16 simpleid2
[root@smzakharoval ~]# id
uid=0(root) gid=0(root) rpytty=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@smzakharoval ~]#
```

Рис. 12: Рис.12. Запуск команд.

```
guest@smzakharoval1:/home/guest
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.3.1 Файл: 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;
}
```

Рис. 13: Рис.13. Запуск команд.

```
[root@smzakharoval ~]# gcc readfile.c -o readfile
[root@smzakharoval ~]#
```

Рис. 14: Рис.14. Компиляция.

```
[root@smzakharoval ~]# chmod 000 readfile.c
[root@smzakharoval ~]#
```

Рис. 15: Рис.15. Изменение прав.

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

```
[root@smzakharoval guest]# su guest
[guest@smzakharoval ~]$ gcc readfile.c -o readfile
cc1: фатальная ошибка: readfile.c: Отказано в доступе
компиляция прервана.
[guest@smzakharoval ~]$ █
```



```
[guest@smzakharova1 ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 12 16:39 /tmp/file01.txt
[guest@smzakharova1 ~]$ chmod o+rw /tmp/file01.txt
[guest@smzakharova1 ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 12 16:39 /tmp/file01.txt
[guest@smzakharova1 ~]$ █
```

Рис. 22: Рис.22. Проверка атрибута и изменение прав.

```
[root@smzakharova1 guest]# su guest2
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test
[guest2@smzakharova1 guest]$ █
```

Рис. 23: Рис.23. Попытка чтения.

слово test3 командой echo "test3" > /tmp/file01.txt. Выполнить операцию удалось (рис.26).

27. Проверила содержимое файла командой cat /tmp/file01.txt (рис.27).

28. От пользователя guest2 попробовала удалить файл /tmp/file01.txt с помощью команды rm /tmp/file01.txt. Удалить файл не удалось (рис.28).

29. Повысила свои права до суперпользователя командой su - и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp (рис.29).

30. Покинула режим суперпользователя командой exit (рис.30).

31. От пользователя guest2 проверил, что атрибута t у директории /tmp нет (рис.31).

32. Повторила предыдущие шаги. Никаких изменений не произошло (рис.32).

```
[guest2@smzakharova1 guest]$ echo "test2" > /tmp/file01.txt
[guest2@smzakharova1 guest]$ █
```

Рис. 24: Рис.24. Изменение информации в файле.

```
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test2
[guest2@smzakharova1 guest]$ █
```

Рис. 25: Рис.25. Проверка содержимого.

```
[guest2@smzakharova1 guest]$ echo "test3" > /tmp/file01.txt
[guest2@smzakharova1 guest]$ █
```

Рис. 26: Рис.26. Изменение информации в файле.

```
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharova1 guest]$ █
```

Рис. 27: Рис.27. Проверка содержимого.

```
[guest2@smzakharova1 guest]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: операция не позволена
[guest2@smzakharova1 guest]$ █
```

Рис. 28: Рис.28. Попытка удаления.

```
[guest2@smzakharova1 guest]$ su
Пароль:
[root@smzakharova1 guest]# chmod -t /tmp
[root@smzakharova1 guest]# █
```

Рис. 29: Рис.29. Повышение прав и снятие атрибута.

```
[root@smzakharova1 guest]# exit
exit
[guest2@smzakharova1 guest]$
```

Рис. 30: Рис.30. Выход из режима суперпользователя.

```
[guest2@smzakharova1 guest]$ ls -l / | grep tmp
drwxrwxrwx. 24 root root 4096 ноя 12 16:39 tmp
[guest2@smzakharova1 guest]$ █
```

Рис. 31: Рис.31. Проверка на наличие атрибута.

```
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharova1 guest]$ echo "test2" > /tmp/file01.txt
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test2
[guest2@smzakharova1 guest]$ echo "test3" > /tmp/file01.txt
[guest2@smzakharova1 guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharova1 guest]$ █
```

Рис. 32: Рис.32. Дублирование предыдущих шагов.

33. Проверила, удалось ли удалить файл от имени пользователя, не являющегося его владельцем? Удалось (рис.33).

```
[guest2@smzakharoval guest]$ rm /tmp/file01.txt  
[guest2@smzakharoval guest]$ █
```

Рис. 33: Рис.33. Проверка удаления.

34. Повысила свои права до суперпользователя с помощью команды su - и вернула атрибут t на директорию /tmp (рис.34).

```
[~guest2@smzakharoval ~guest]$ su  
Пароль:  
[root@smzakharoval guest]# chmod +t /tmp  
[root@smzakharoval guest]# exit  
exit  
[guest2@smzakharoval guest]$ █
```

Рис. 34: Рис.34. Установка атрибута.

Вы-
во-
ды

Благодаря

дан-
ной

ла-
бо-

ра-
тор-
ной

ра-
бо-

те, я

изу-
чил

ме-
ха-

низ-
мы

из-
ме-

не-
ния

иден-
ти-

фи-
ка-

то-
ров,

при-
ме-

не-
ния

SetUID-

и

Sticky-
битов.

По-
лу-

чил
прак-

ти-
че-

ские

на-
вы-

ки
ра-

бо-
12
ты в

кон-
соли

с до-
пол-

ни-
тель-

ны-

==

Спасибо за внимание!