

Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния
дополнительных атрибутов

Захарова Софья Михайловна

Оглавление

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	18

Список таблиц

Список иллюстраций

0.1	Рис.1. Вход в систему.	7
0.2	Рис.2. Создание программы.	7
0.3	Рис.3. Компиляция файла.	8
0.4	Рис.4. Выполнение программы.	8
0.5	Рис.5. Выполнение программы и сравнение с предыдущей.	8
0.6	Рис.6. Усложнение программы.	9
0.7	Рис.7. Компиляция и запуск второй программы.	9
0.8	Рис.8. Выполнение команд.	10
0.9	Рис.9. Повышение прав.	10
0.10	Рис.10. Проверка.	10
0.11	Рис.11. Запуск команд.	10
0.12	Рис.12. Запуск команд.	11
0.13	Рис.13. Запуск команд.	11
0.14	Рис.14. Компиляция.	11
0.15	Рис.15. Изменение прав.	12
0.16	Рис.16. Проверка.	12
0.17	Рис.17. Изменение прав.	12
0.18	Рис.18. Проверка.	12
0.19	Рис.19. Проверка.	13
0.20	Рис.20. Проверка наличия атрибута.	13
0.21	Рис.21. Создание файла.	13
0.22	Рис.22. Проверка атрибута и изменение прав.	14
0.23	Рис.23. Попытка чтения.	14
0.24	Рис.24. Изменение информации в файле.	14
0.25	Рис.25. Проверка содержимого.	14
0.26	Рис.26. Изменение информации в файле.	15
0.27	Рис.27. Проверка содержимого.	15
0.28	Рис.28. Попытка удаления.	15
0.29	Рис.29. Повышение прав и снятие атрибута.	15
0.30	Рис.30. Выход из режима суперпользователя.	16
0.31	Рис.31. Проверка на наличие атрибута.	16
0.32	Рис.32. Дублирование предыдущих шагов.	16
0.33	Рис.33. Проверка удаления.	16
0.34	Рис.34. Установка атрибута.	17

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.

Задание

Лабораторная работа подразумевает работу с виртуальной машиной VirtualBox, операционной системой Linux, дистрибутивом Centos и закрепление теоретических основ получения практических навыков работы в консоли с атрибутами файлов.

Выполнение лабораторной работы

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

A terminal window showing the login prompt [guest@smzakharoval ~]\$ in a monospaced font. The background is light gray, and the text is dark gray.

Рис. 0.1: Рис.1. Вход в систему.

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

A screenshot of the GNU nano 2.3.1 text editor. The title bar shows 'guest@smzakharoval:~'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The status bar shows 'GNU nano 2.3.1' and 'Файл: simpleid.c'. The editor contains the following C code:

```
#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;
}
```

A cursor is visible at the end of the closing brace on the last line.

Рис. 0.2: Рис.2. Создание программы.

Скомпилировала программу и убедилась, что файл программы создан: “gcc simpleid.c -o simpleid” (рис.3).

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

Рис. 0.3: Рис.3. Компиляция файла.

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

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

Рис. 0.4: Рис.4. Выполнение программы.

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.c1023
[guest@smzakharoval ~]$ █
```

Рис. 0.5: Рис.5. Выполнение программы и сравнение с предыдущей.

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


```
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 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. 0.6: Рис.6. Усложнение программы.

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

```
[guest@smzakharova1 ~]$ gcc simpleid2.c -o simpleid2  
[guest@smzakharova1 ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@smzakharova1 ~]$
```

Рис. 0.7: Рис.7. Компиляция и запуск второй программы.

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@smzakharova1 ~]$ su
Пароль:

[root@smzakharova1 guest]#
[root@smzakharova1 guest]# chown root:guest /home/guest/simpleid2
[root@smzakharova1 guest]# chmod u+s /home/guest/simpleid2
[root@smzakharova1 guest]# █
```

Рис. 0.8: Рис.8. Выполнение команд.

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

```
[guest@smzakharova1 ~]$ su
Пароль:
```

Рис. 0.9: Рис.9. Повышение прав.

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

```
[root@smzakharova1 guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8656 ноя 12 16:16 simpleid2
[root@smzakharova1 guest]# █
```

Рис. 0.10: Рис.10. Проверка.

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

```
[root@smzakharova1 guest]# ./simpleid2
e uid=0, e gid=0
real uid=0, real gid=0
[root@smzakharova1 guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
[root@smzakharova1 guest]# █
```

Рис. 0.11: Рис.11. Запуск команд.

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

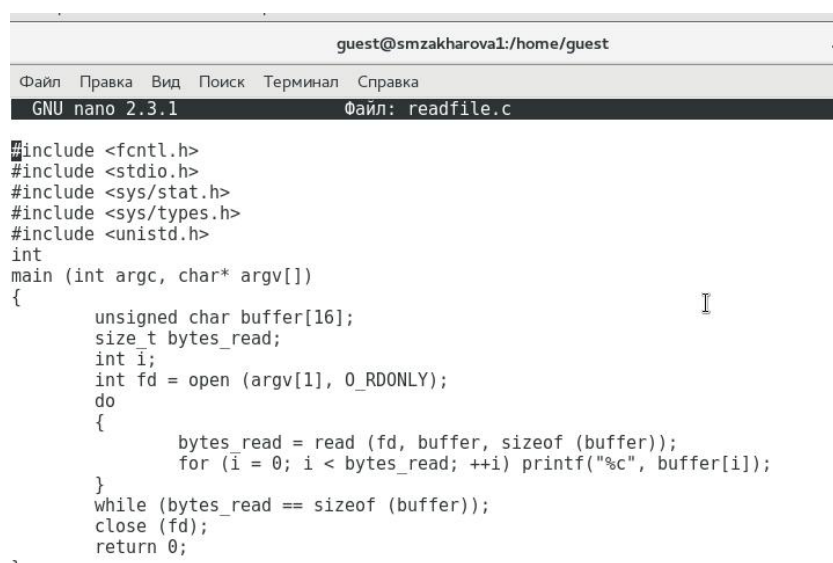
```

[root@smzakharova1 guest]# chown root:guest /home/guest/simpleid2
[root@smzakharova1 guest]# chmod u+s /home/guest/simpleid2
[root@smzakharova1 guest]# chmod g+s /home/guest/simpleid2
[root@smzakharova1 guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 8656 ноя 12 16:16 simpleid2
[root@smzakharova1 guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@smzakharova1 guest]#

```

Рис. 0.12: Рис.12. Запуск команд.

Создала программу readfile.c (рис.13).



```

guest@smzakharova1:/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. 0.13: Рис.13. Запуск команд.

Откомпилировала её (рис.14).

```

[root@smzakharova1 guest]# gcc readfile.c -o readfile
[root@smzakharova1 guest]#

```

Рис. 0.14: Рис.14. Компиляция.

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

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

```
[guest@smzakharoval ~]$ ./readfile /etc/shadow
jQ{00LB005000x86_64./readfile/etc/shadowXDG_VTNR=1SSH_AGENT_PID=1958XDG_SESSION_ID=1H
OSTNAME=smzakharoval.localdomainIMSETTINGS_INTEGRATE_DESKTOP=yesTERM=xterm-256colorSHEL
L=/bin/bashXDG_MENU_PREFIX=gnome-VTE VERSION=4602HISTSIZE=1000GJS_DEBUG_OUTPUT=stderrWI
NDOWID=46137350GJS_DEBUG_TOPICS=JS ERROR;JS LOGIMSETTINGS_MODULE=X compose tableUSER=gu
estLS_COLORS=rs=0:di=38;5;27:ln=38;5;51:mh=44;38;5;15:pi=40;38;5;11:so=38;5;13:do=38;5;
5:bd=48;5;232;38;5;11:cd=48;5;232;38;5;3:or=48;5;232;38;5;9:mi=05;48;5;232;38;5;15:su=4
8;5;196;38;5;15:sg=48;5;11;38;5;16:ca=48;5;196;38;5;226:tw=48;5;10;38;5;16:ow=48;5;10;3
8;5;21:st=48;5;21;38;5;15:ex=38;5;34:*.tar=38;5;9:*.tgz=38;5;9:*.arc=38;5;9:*.arj=38;5;
9:*.taz=38;5;9:*.lha=38;5;9:*.lz4=38;5;9:*.lzh=38;5;9:*.lzma=38;5;9:*.tlz=38;5;9:*.txz=
38;5;9:*.tzo=38;5;9:*.t7z=38;5;9:*.zip=38;5;9:*.z=38;5;9:*.Z=38;5;9:*.dz=38;5;9:*.gz=3
8;5;9:*.lrz=38;5;9:*.lz=38;5;9:*.lzo=38;5;9:*.xz=38;5;9:*.bz2=38;5;9:*.bz=38;5;9:*.tbz=3
8;5;9:*.tbz2=38;5;9:*.tz=38;5;9:*.deb=38;5;9:*.rpm=38;5;9:*.jar=38;5;9:*.war=38;5;9:*.e
ar=38;5;9:*.sar=38;5;9:*.rar=38;5;9:*.alz=38;5;9:*.ace=38;5;9:*.zoo=38;5;9:*.cpio=38;5;
9:*.7z=38;5;9:*.rz=38;5;9:*.cab=38;5;9:*.jpg=38;5;13:*.jpeg=38;5;13:*.gif=38;5;13:*.bmp
```

Рис. 0.19: Рис.19. Проверка.

Исследование Sticky-бита

Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду `ls -l / | grep tmp` (рис.20).

```
[guest@smzakharoval ~]$ ls -l / | grep tmp
drwxrwxrwt. 24 root root 4096 ноя 12 16:35 tmp
[guest@smzakharoval ~]$
```

Рис. 0.20: Рис.20. Проверка наличия атрибута.

От имени пользователя guest создала файл file01.txt в директории /tmp со словом `test: echo & quot;test& quot; & gt; /tmp/file01.txt` (рис.21).

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

Рис. 0.21: Рис.21. Создание файла.

Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные». Первоначально все груп-

пы имели право на чтение, а запись могли осуществлять все, кроме «остальных пользователей» (рис.22).

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

Рис. 0.22: Рис.22. Проверка атрибута и изменение прав.

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

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

Рис. 0.23: Рис.23. Попытка чтения.

От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2, стерев при этом всю имеющуюся в файле информацию с помощью команды echo "test2" & gt; /tmp/file01.txt. Выполнить операцию удалось (рис.24).

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

Рис. 0.24: Рис.24. Изменение информации в файле.

Проверила содержимое файла командой cat /tmp/file01.txt (рис.25).

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

Рис. 0.25: Рис.25. Проверка содержимого.

От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test3 командой `echo "test3" > /tmp/file01.txt`. Выполнить операцию удалось (рис.26).

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

Рис. 0.26: Рис.26. Изменение информации в файле.

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

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

Рис. 0.27: Рис.27. Проверка содержимого.

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

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

Рис. 0.28: Рис.28. Попытка удаления.

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).

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

Рис. 0.29: Рис.29. Повышение прав и снятие атрибута.

Покинула режим суперпользователя командой exit (рис.30).

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

Рис. 0.30: Рис.30. Выход из режима суперпользователя.

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

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

Рис. 0.31: Рис.31. Проверка на наличие атрибута.

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

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

Рис. 0.32: Рис.32. Дублирование предыдущих шагов.

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. 0.33: Рис.33. Проверка удаления.

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


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

Рис. 0.34: Рис.34. Установка атрибута.

Выводы

Благодаря данной лабораторной работе, 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.