

Лабораторная работа №5

**Дискреционное разграничение прав в Linux. Исследование
влияния дополнительных атрибутов**

Крутова Екатерина Дмитриевна

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	14

Список иллюстраций

1	Вход в систему от имени пользователя guest	6
2	Создание программы simpleid.c	6
3	simpleid.c	6
4	Компиляция программы simpleid.c	7
5	Выполнение программы simpleid.c	7
6	Выполнение системной программы id	7
7	simpleid2.c	7
8	Компиляция и выполнение	8
9	Выполнение команд по изменению владельца файла и установке SetU'D-бита	8
10	Проверка установки атрибутов	8
11	Выполнение simpleid2 и id	8
12	readfile.c	9
13	Компиляция	9
14	Изменение владельца и прав	9
15	Попытка прочитать файл readfile.c	9
16	Изменение владельца и установка SetU'D-бита	9
17	Попытка прочитать файл readfile.c (неуспешно)	10
18	Попытка прочитать файл /etc/shadow (неуспешно)	10
19	Проверка, установлен ли атрибут Sticky на директории /tmp	11
20	Создание файла file01.txt в директории /tmp	11
21	Просмотр атрибутов и изменение прав	11
22	Попытка прочитать файл	11
23	Попытка дозаписать в файл /tmp/file01.txt слово test2 (отказ в доступе)	11
24	Чтение файла	11
25	Попытка записать в файл /tmp/file01.txt слово test3	12
26	Чтение файла	12
27	Попытка удалить файл /tmp/file01.txt	12
28	Изменение прав	12
29	Снятие режима суперпользователя	12
30	Проверка атрибутов	13
31	Попытка изменить файл (неуспешно), удалить файл (успешно)	13
32	Возвращение атрибута	13

Список таблиц

Цель работы

Целью данной работы является 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

1. Создание программы (рис. [-@fig:001] - [-@fig:018]).

```
[edkrutova@edkrutova ~]$ su guest
Password:
[guest@edkrutova edkrutova]$
```

Рис. 1: Вход в систему от имени пользователя guest

```
[guest@edkrutova ~]$ touch simpleid.c
[guest@edkrutova ~]$
```

Рис. 2: Создание программы simpleid.c

```
simpleid.c      [-M--] 11 L:[ 1+ 8 9/
#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. 3: simpleid.c

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

Рис. 4: Компиляция программы simpleid.c

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

Рис. 5: Выполнение программы simpleid.c

```
[guest@edkrutova ~]$ ./simpleid
uid=1001, gid=1001
[guest@edkrutova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@edkrutova ~]$
```

Рис. 6: Выполнение системной программы id

Вывод идентичен.

```
[simpleid2.c] [-M--]
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t real_uid = geteuid();
    gid_t real_gid = getegid();
    uid_t e_uid = geteuid();
    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. 7: simpleid2.c

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

Рис. 8: Компиляция и выполнение

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

Рис. 9: Выполнение команд по изменению владельца файла и установке SetU'D-бита

```
[root@edkrutova ~]# ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 17616 Oct  5 12:24 /home/guest/simpleid2
[root@edkrutova ~]#
```

Рис. 10: Проверка установки атрибутов

```
[guest@edkrutova ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=1001
[guest@edkrutova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@edkrutova ~]$
```

Рис. 11: Выполнение simpleid2 и id


```

[readline.c] [-M--] [*]
#include <fcntl.h>
#include <sys/stat.h>
#include <stdio.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;
}
17 18/23 313/436 [00032 0x0020]

```

Рис. 12: readfile.c

```

[guest@edkrutova ~]$ gcc readline.c -o readline
[guest@edkrutova ~]$

```

Рис. 13: Компиляция

```

[root@edkrutova guest]# chown root:guest /home/guest/readline.c
[root@edkrutova guest]# chmod 000 readline.c
[root@edkrutova guest]#

```

Рис. 14: Изменение владельца и прав

```

}[guest@edkrutova ~]$ cat readline.c
cat: readline.c: Permission denied
[guest@edkrutova ~]$

```

Рис. 15: Попытка прочитать файл readfile.c

```

[root@edkrutova guest]# chown guest:root /home/guest/readline.c
[root@edkrutova guest]# chmod u+s /home/guest/readline.c
[root@edkrutova guest]#

```

Рис. 16: Изменение владельца и установка SetU'D-бита

```
[root@edkrutova guest]# ./readline readline.c
#include <sys/types.h>
#include <unistd.h>
#include <fcntl.h>
#include <sys/stat.h>
#include <stdio.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;
}[root@edkrutova guest]#
```

Рис. 17: Попытка прочитать файл readline.c (неуспешно)

```
[guest@edkrutova ~]$ ./readline /etc/shadow
v@eZ 6i
v@eZ 6i
CN
3iON
86_64./readline/etc/shadowSHELL=/bin/bashSESSION
N_MANAGER=local/unix:@/tmp/.ICE-unix/2184,unix/unix:/tmp/.ICE-unix/2184COLORTERM
=truecolorHISTCONTROL=ignoredupsXDG_MENU_PREFIX=gnome-HOSTNAME=edkrutovaHISTSIZE
=1000SSH_AUTH_SOCK=/run/user/1000/keyring/sshXMODIFIERS=@im=ibusDESKTOP_SESSION=
gnomePWD=/home/guestXDG_SESSION_DESKTOP=gnomeLOGNAME=guestXDG_SESSION_TYPE=wayla
ndSYSTEMD_EXEC_PID=2202XAUTHORITY=/home/guest/.xauthEQ0yU3GDM_LANG=en_US.UTF-8HO
ME=/home/guestUSERNAME=edkrutovaLANG=en_US.UTF-8LS_COLORS=rs=0:di=01;34:ln=01;36
:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;37;4
1:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.t
gz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31
:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01
;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01
;31:*.tazst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.de
b=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:
*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mj
pg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;
35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.sv
g=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;3
5:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.m4
v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:
```

Рис. 18: Попытка прочитать файл /etc/shadow (неуспешно)

2. Исследование Sticky-бита (рис. [-@fig:019] - [-@fig:032]).

```
[guest@edkrutova ~]$ ls -l | grep tmp
[guest@edkrutova ~]$
```

Рис. 19: Проверка, установлен ли атрибут Sticky на директории /tmp

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

Рис. 20: Создание файла file01.txt в директории /tmp

```
[guest@edkrutova ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  5 12:56 /tmp/file01.txt
[guest@edkrutova ~]$ chmod o+rw /tmp/file01.txt
[guest@edkrutova ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  5 12:56 /tmp/file01.txt
[guest@edkrutova ~]$
```

Рис. 21: Просмотр атрибутов и изменение прав

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

Рис. 22: Попытка прочитать файл

```
[guest2@edkrutova edkrutova]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@edkrutova edkrutova]$
```

Рис. 23: Попытка дозаписать в файл /tmp/file01.txt слово test2 (отказ в доступе)

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

Рис. 24: Чтение файла

```
[guest2@edkrutova edkrutova]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@edkrutova edkrutova]$
```

Рис. 25: Попытка записать в файл /tmp/file01.txt слово test3

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

Рис. 26: Чтение файла

```
[guest2@edkrutova edkrutova]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@edkrutova edkrutova]$
```

Рис. 27: Попытка удалить файл /tmp/file01.txt

```
[guest2@edkrutova edkrutova]$ su -
Password:
[root@edkrutova ~]# chmod -t /tmp/
[root@edkrutova ~]#
```

Рис. 28: Изменение прав

```
[root@edkrutova ~]# exit
logout
[guest2@edkrutova edkrutova]$
```

Рис. 29: Снятие режима суперпользователя

```
[guest2@edkrutova edkrutova]$ ls -l | grep tmp
ls: cannot open directory '.': Permission denied
[guest2@edkrutova edkrutova]$
```

Рис. 30: Проверка атрибутов

```
[guest2@edkrutova edkrutova]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@edkrutova edkrutova]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@edkrutova edkrutova]$
```

Рис. 31: Попытка изменить файл (неуспешно), удалить файл (успешно)

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

Рис. 32: Возвращение атрибута

Выводы

Я изучила механизмов изменения идентификаторов, применения SetUID- и Sticky-битов, получила практические навыки работы в консоли с дополнительными атрибутами, рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.