

Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Аксёнова Алина Владимировна

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.

Ход работы

Написание, запуск и результат работы первой программы

```
guest@avaksenova:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@avaksenova ~]$ nano simpleid.c  
[guest@avaksenova ~]$ gcc simpleid.c -o simpleid  
[guest@avaksenova ~]$ ls -l  
итого 16  
drwxrwxrwx. 2 guest guest   19 окт 27 22:21 dir1  
-rwxrwxr-x. 1 guest guest 8472 ноя 12 15:49 simpleid  
-rw-rw-r--. 1 guest guest  175 ноя 12 15:48 simpleid.c  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Видео  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Документы  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Загрузки  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Изображения  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Музыка  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Общедоступные  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Рабочий стол  
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Шаблоны  
[guest@avaksenova ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@avaksenova ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@avaksenova ~]$
```

Написание, запуск и результат работы второй программы

```
[guest@avaksenova ~]$ nano simpleid2.c
[guest@avaksenova ~]$ gcc
gcc          gcc-ar      gcc-nm      gcc-ranlib
[guest@avaksenova ~]$ gcc simpleid2.c -o simpleid2
[guest@avaksenova ~]$ ls -l
итого 32
drwxrwxrwx. 2 guest guest   19 окт 27 22:21 dir1
-rwxrwxr-x. 1 guest guest 8472 ноя 12 15:49 simpleid
-rwxrwxr-x. 1 guest guest 8576 ноя 12 15:53 simpleid2
-rw-rw-r--. 1 guest guest  313 ноя 12 15:53 simpleid2.c
-rw-rw-r--. 1 guest guest  175 ноя 12 15:48 simpleid.c
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Видео
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Документы
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Загрузки
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Изображения
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Музыка
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Общедоступные
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Рабочий стол
drwxr-xr-x. 2 guest guest    6 окт  1 16:23 Шаблоны
[guest@avaksenova ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@avaksenova ~]$ █
```

Смена владельца и установление SetUID-бита на программу simpleid2

```
root@avaksenova:~  
[guest@avaksenova ~]$ su -  
Пароль:  
Последний вход в систему: Пт ноя 12 15:37:11 MSK 2021 на pts/0  
[root@avaksenova ~]# chown root:guest /home/guest/simpleid2  
[root@avaksenova ~]# chmod u+s /home/guest/simpleid2  
[root@avaksenova ~]# pwd  
/root
```

```
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Загрузки  
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Изображения  
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Музыка  
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Рабочий стол  
drwxr-xr-x. 2 guest guest 6 окт 1 16:23 Шаблоны  
[guest@avaksenova ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@avaksenova ~]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest 8576 ноя 12 15:53 simpleid2  
[guest@avaksenova ~]$ ./simpleid2
```

```
[root@avaksenova guest]# chmod 777 readfile  
[root@avaksenova guest]# chown root:guest /home/guest/readfile.c  
[root@avaksenova guest]# chmod 700 readfile.c  
[root@avaksenova guest]#
```

Чтение файла readfile.c программой readfile

```
guest@avaksenova:~  
Файл Правка Вид Поиск Терминал Справка  
stat: readfile.c: Отказано в доступе  
guest@avaksenova ~]$ ./readfile 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;  
}  
guest@avaksenova ~]$ ./readfile /etc/shadow
```


Проверка файла в директории со Sticky-битом

```
[guest@avaksenova ~]$ ls -l / | grep tmp
drwxrwxrwt. 15 root root 4096 ноя 12 16:24 tmp
[guest@avaksenova ~]$ cd /tmp
[guest@avaksenova tmp]$ touch file01.txt
[guest@avaksenova tmp]$ echo "test" > /tmp/file01.txt
[guest@avaksenova tmp]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 12 16:26 /tmp/file01.txt
[guest@avaksenova tmp]$ chmod o+rw /tmp/file01.txt
[guest@avaksenova tmp]$ chmod o+rw /tmp/file01.txt
[guest@avaksenova tmp]$ ls -l /tmp/file01.tx
ls: невозможно получить доступ к /tmp/file01.tx: Нет такого файла или каталога
[guest@avaksenova tmp]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ноя 12 16:26 /tmp/file01.txt
[guest@avaksenova tmp]$ █
```

Проверка файла в директории без Sticky-бита

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@avaksenova ~]$ su guest2
Пароль:
[guest2@avaksenova guest]$ cat /tmp/file01.tx
cat: /tmp/file01.tx: Нет такого файла или каталога
[guest2@avaksenova guest]$ cat /tmp/file01.txt
test
[guest2@avaksenova guest]$ echo "test2" >> /tmp/file01.txt
[guest2@avaksenova guest]$ cat /tmp/file01.txt
test
test2
[guest2@avaksenova guest]$ echo "test3" > /tmp/file01.txt
[guest2@avaksenova guest]$ cat /tmp/file01.txt
test3
[guest2@avaksenova home]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Нет такого файла или каталога
[guest2@avaksenova home]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Нет такого файла или каталога
[guest2@avaksenova home]$ rm /tmp/file01.txt
[guest2@avaksenova home]$ ls -l
итого 8
drwx-----. 15 avaksenova avaksenova 4096 окт  1 15:54 avaksenova
drwxrwx----. 16 guest      guest      4096 ноя 12 16:18 guest
drwx-----.  5 guest2     guest2     148  ноя 12 16:28 guest2
[guest2@avaksenova home]$
```

- В результате выполнения данной работы были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Кроме того, получены практические навыки работы в консоли с дополнительными атрибутами, рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.