Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Рыбалко Элина[1]

2022, 03 September, 2022 Moscow, Russian Federation

[1]RUDN University, Moscow, Russian Federation

Прагматика выполнения лабораторной работы

- Приобретение практических навыков работы с атрибутами, дискреционным разграничением прав и механизмами изменения идентификаторов на операционной системы Linux.

Цель выполнения лабораторной работы

Изучить механизмы 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.

Задачи выполнения лабораторной работы

- Подготовка лабораторного стенда.
- Создание и компиляция программы.
- Исследование Sticky-бита.

Результаты выполнения лабораторной работы

```
[eprybalko@eprybalko ~]$ su
Пароль:
[root@eprybalko eprybalko]# yum install gcc
Загружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.corbina.net
 * extras: mirror.corbina.net
 * updates: mirror.corbina.net
Пакет gcc-4.8.5-44.el7.x86_64 уже установлен, и это последняя версия.
Выполнять нечего
[root@eprybalko eprybalko]# setenforce 0
[root@eprybalko eprybalko]# getenforce
Permissive
```

Рис. 1: Подготовка лабораторного стенда

Результаты выполнения лабораторной работы

guest@eprybalko:~

Файл Правка Вид Поиск Терминал Справка

```
#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: Создание программы simpleid.c

Результаты выполнения лабораторной работы

```
[guest@eprybalko ~]$ vim simpleid.c
[guest@eprybalko ~]$ gcc simpleid.c -o simpleid
[guest@eprybalko ~]$ ./simpleid
uid=1001, gid=1001
[guest@eprybalko ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned r:unconfined t:s0-s0:c0.c1023
```

Рис. 3: Компиляция программы simpleid.c

Результаты выполнения лабораторной работы

```
[guest@eprybalko ~]$ gcc simpleid2.c -o simpleid2
[guest@eprybalko ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@eprybalko ~]$ su
Пароль:
[root@eprybalko guest]# chown root:guest /home/guest/simpleid2
[root@eprybalko guest]# chmod u+s /home/guest/simpleid2
[root@eprybalko guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 8616 окт  2 22:20 simpleid2
[root@eprybalko guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@eprybalko guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
[root@eprybalko guest]# chmod g+s /home/guest/simpleid2
[root@eprybalko guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 8616 окт  2 22:20 simpleid2
[root@eprybalko guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
```

Рис. 4: Компиляция simpleid2.c и изменение прав

Результаты выполнения лабораторной работы

```
[root@eprybalko guest]# vim readfile.c
[root@eprybalko guest]# gcc readfile.c -o readfile
[root@eprybalko guest]# chown root readfile.c
[root@eprybalko guest]# chmod og-rwx readfile.c
[root@eprybalko guest]# exit
exit
[guest@eprybalko ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@eprybalko ~]$ su
Пароль:
[root@eprybalko guest]# chmod u+s /home/guest/readfile
```

Рис. 5: Компиляция readfile.c и изменение прав

Результаты выполнения лабораторной работы

```
[guest@eprybalko ~]$ ./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;
}
```

Рис. 6: Проверка чтения файла readfile.c

Результаты выполнения лабораторной работы

```
[guest@eprybalko ~]$ ls -l / | grep tmp
drwxrwxrwt.  18 root root 4096 окт  2 23:54 tmp
[guest@eprybalko ~]$ echo "test" > /tmp/file01.txt
[guest@eprybalko ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 окт  2 23:55 /tmp/file01.txt
[guest@eprybalko ~]$ chmod o+rw /tmp/file01.txt
[guest@eprybalko ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  2 23:55 /tmp/file01.txt
[guest@eprybalko ~]$ su guest2
Пароль:
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test
[guest2@eprybalko guest]$ echo "test2" > /tmp/file01.txt
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test2
[guest2@eprybalko guest]$ echo "test3" > /tmp/file01.txt
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test3
[guest2@eprybalko guest]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Операция не позволена
[guest2@eprybalko guest]$ su -
Пароль:
Последний вход в систему:Вс окт  2 22:38:33 MSK 2022на pts/1
[root@eprybalko ~]# chmod -t /tmp
[root@eprybalko ~]# exit
logout
```

Рис. 7: Чтение и запись файла с атрибутом Sticky-бит

Результаты выполнения лабораторной работы

```
[guest2@eprybalko guest]$ ls -l / | grep tmp
drwxrwxrwx.  18 root root 4096 окт  2 23:59 tmp
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test3
[guest2@eprybalko guest]$ echo "test2" > /tmp/file01.txt
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test2
[guest2@eprybalko guest]$ echo "test3" > /tmp/file01.txt
[guest2@eprybalko guest]$ cat /tmp/file01.txt
test3
[guest2@eprybalko guest]$ rm /tmp/file01.txt
[guest2@eprybalko guest]$ su -
Пароль:
Последний вход в систему:Вс окт  2 23:59:30 MSK 2022на pts/1
[root@eprybalko ~]# chmod +t /tmp
[root@eprybalko ~]# exit
logout
[guest2@eprybalko guest]$ ls -l / | grep tmp
drwxrwxrwt.  19 root root 4096 окт  3 00:01 tmp
```

Рис. 8: Чтение и запись файла без атрибута Sticky-бит

Вывод

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.