

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Алиев Расул НБИ-01-19

5 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

Цель лабораторной 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.

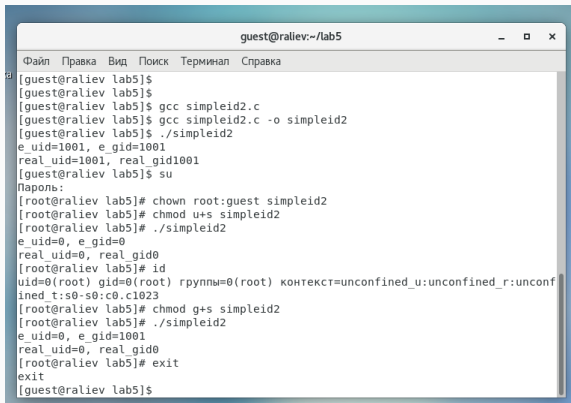
Выполнение лабораторной работы

Программа simpleid

```
-----
[guest@raliev ~]$ mkdir lab5
[guest@raliev ~]$ cd lab5/
[guest@raliev lab5]$ touch simpleid.c
[guest@raliev lab5]$ touch simpleid2.c
[guest@raliev lab5]$ touch readfile.c
[guest@raliev lab5]$ gedit simpleid.c
[guest@raliev lab5]$
[guest@raliev lab5]$ gcc simpleid.c
^[[A[guest@raliev lab5]$ gedit simpleid.c -o simpleid
Неизвестный параметр -o
[guest@raliev lab5]$ gcc simpleid.c -o simpleid
[guest@raliev lab5]$ ./simpleid
uid=1001, gid=1001
[guest@raliev lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined t:s0-s0:c0.c1023
[guest@raliev lab5]$ █
```

Figure 1: результат программы simpleid

Программа simpleid2



```
guest@raliev:~/lab5
Файл Правка Вид Поиск Терминал Справка
[guest@raliev lab5]$
[guest@raliev lab5]$
[guest@raliev lab5]$ gcc simpleid2.c
[guest@raliev lab5]$ gcc simpleid2.c -o simpleid2
[guest@raliev lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@raliev lab5]$ su
Пароль:
[root@raliev lab5]# chown root:guest simpleid2
[root@raliev lab5]# chmod u+s simpleid2
[root@raliev lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@raliev lab5]# id
uid=0(root) gid=0(root) rгруппы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@raliev lab5]# chmod g+s simpleid2
[root@raliev lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@raliev lab5]# exit
exit
[guest@raliev lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

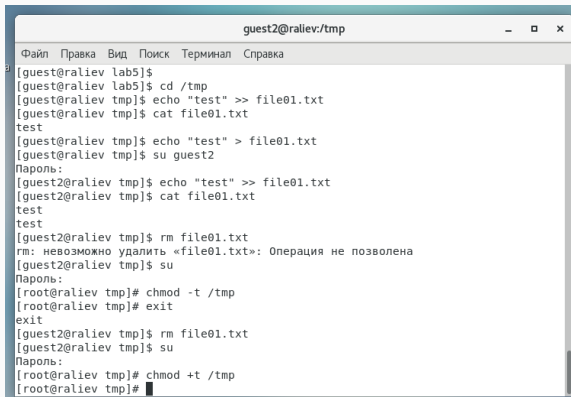
```

guest@raliev: ~/lab5
Файл  Правка  Вид  Поиск  Терминал  Справка
0150623 (Red Hat 4.8.5-44)
crtdyn.o crtstuff.c JCR LIST deregister_tm_clones do_global_dtors_
auxcompleted.6355 do_global_dtors_aux fini_array_entryframe dummy_frame dummy_
init_array_entryreadfile.c FRAME END JCR END init_array_end DYNAMIC init_
_array_start GNU EH FRAME HDR GLOBAL OFFSET TABLE libc csu finiupchar@GLIBC
2.2.5 edataclose@GLIBC 2.2.5 read@GLIBC 2.2.5 libc start main@GLIBC 2.2.5 d
ata start gmon start dso handle ld_stdin_used libc csu init_bss startmaino
pen@GLIBC 2.2.5 TMC END _symtab.strtab.shstrtab.interp.note.ABI-tag.note.gnu.
build-id.gnu.hash.dynsym.dynstr.gnu.version.gnu.version_r.rela.dyn.rela.plt.init
.text.fini.rodata.eh_frame_hdr.eh_frame.init_array.fini_array.jcr.dynamic.got.go
t.plt.data.bss.comment
cat: readfile.c: Отказано в доступе
[guest@raliev lab5]$ ./readfile.readfile.c
#include <stdio.h>
main()
{
    FILE *f;
    char *s;
    s = "readfile.c";
    f = fopen(s, "r");
    if (f == NULL)
    {
        printf("File %s not found\n", s);
        return 1;
    }
    while ((s = fgets(s, 1024, f)) != NULL)
    {
        printf("%s", s);
    }
    fclose(f);
    return 0;
}

```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
guest2@raliev: /tmp
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@raliev lab5]$
[guest@raliev lab5]$ cd /tmp
[guest@raliev tmp]$ echo "test" >> file01.txt
[guest@raliev tmp]$ cat file01.txt
test
[guest@raliev tmp]$ echo "test" > file01.txt
[guest@raliev tmp]$ su guest2
Пароль:
[guest2@raliev tmp]$ echo "test" >> file01.txt
[guest2@raliev tmp]$ cat file01.txt
test
test
[guest2@raliev tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@raliev tmp]$ su
Пароль:
[root@raliev tmp]# chmod -t /tmp
[root@raliev tmp]# exit
exit
[guest2@raliev tmp]$ rm file01.txt
[guest2@raliev tmp]$ su
Пароль:
[root@raliev tmp]# chmod +t /tmp
[root@raliev tmp]#
```

Figure 4: исследование Sticky-бита

Выводы

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