

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ростислав Арзуманян НБИ-01-20

28 сентября, 2023, 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@rharzumanyan ~]$  
[guest@rharzumanyan ~]$ mkdir lab5  
[guest@rharzumanyan ~]$ cd lab5/  
[guest@rharzumanyan lab5]$ touch simpleid.c  
[guest@rharzumanyan lab5]$ gcc simpleid.c  
[guest@rharzumanyan lab5]$ gcc simpleid.c -o simpleid  
[guest@rharzumanyan lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@rharzumanyan lab5]$ id  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest),10(wheel) контекст=unconfined_u:unconfine  
d_r:unconfined_t:s0-s0:c0.c1023  
[guest@rharzumanyan lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@rharzumanyan lab5]$ touch simpleid2.c
[guest@rharzumanyan lab5]$ gcc simpleid2.c
[guest@rharzumanyan lab5]$ gcc simpleid2.c -o simpleid2.c
gcc: фатальная ошибка: входной файл «simpleid2.c» совпадает с выходным файлом
компиляция прервана.
[guest@rharzumanyan lab5]$ gcc simpleid2.c -o simpleid2
[guest@rharzumanyan lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@rharzumanyan lab5]$ su
Пароль:
[root@rharzumanyan lab5]# chown root:guest simpleid2
[root@rharzumanyan lab5]# chmod u+s simpleid2
[root@rharzumanyan lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@rharzumanyan lab5]# id
uid=0(root) gid=0(root) rpyны=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0
:c0.c1023
[root@rharzumanyan lab5]# chmod g+s simpleid2
[root@rharzumanyan lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@rharzumanyan lab5]#
exit
[guest@rharzumanyan lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@rharzumanyan lab5]$ touch readfile.c
[guest@rharzumanyan lab5]$
[guest@rharzumanyan lab5]$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
   20 | while (bytes_read == (buffer));
      |                   ^~
[guest@rharzumanyan lab5]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
   20 | while (bytes_read == (buffer));
      |                   ^~
[guest@rharzumanyan lab5]$ su
Пароль:
[root@rharzumanyan lab5]# chown root:root readfile
[root@rharzumanyan lab5]# chmod -rwx readfile.c
[root@rharzumanyan lab5]# chmod u+s readfile
[root@rharzumanyan lab5]#
exit
[guest@rharzumanyan lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@rharzumanyan lab5]$ ./readfile readfile.c
#include <stdio.h>
[guest@rharzumanyan lab5]$ ./readfile /etc/shadow
root:$6$0mJpkglj[guest@rharzumanyan lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@rharzumanyan lab5]$  
[guest@rharzumanyan lab5]$ echo test >> /tmp/file01.txt  
[guest@rharzumanyan lab5]$ chmod g+rw /tmp/file01.txt  
[guest@rharzumanyan lab5]$ su guest2  
Пароль:  
[guest2@rharzumanyan lab5]$ cd /tmp/  
[guest2@rharzumanyan tmp]$ cat file01.txt  
test  
[guest2@rharzumanyan tmp]$ echo test >> file01.txt  
bash: file01.txt: Отказано в доступе  
[guest2@rharzumanyan tmp]$ echo test > file01.txt  
bash: file01.txt: Отказано в доступе  
[guest2@rharzumanyan tmp]$ rm file01.txt  
rm: удалить защищённый от записи обычный файл 'file01.txt'? y  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@rharzumanyan tmp]$ su  
Пароль:  
[root@rharzumanyan tmp]# chmod -t /tmp  
[root@rharzumanyan tmp]#  
exit  
[guest2@rharzumanyan tmp]$ echo test >> file01.txt  
bash: file01.txt: Отказано в доступе  
[guest2@rharzumanyan tmp]$ echo test > file01.txt  
bash: file01.txt: Отказано в доступе  
[guest2@rharzumanyan tmp]$ rm file01.txt  
rm: удалить защищённый от записи обычный файл 'file01.txt'? y  
[guest2@rharzumanyan 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.