

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ахаян Анаида НБИ-01-19

6 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

```
Permissive
[guest@aaahayan ~]$ mkdir lab5
[guest@aaahayan ~]$ cd lab5
[guest@aaahayan lab5]$ touch simoleid.c
[guest@aaahayan lab5]$ touch simoleid2.c
[guest@aaahayan lab5]$ touch readfile.c
[guest@aaahayan lab5]$ gedit simoleid.c
[guest@aaahayan lab5]$ gcc simoleid.c
[guest@aaahayan lab5]$ gcc simoleid.c -o simoleid
[guest@aaahayan lab5]$ ./simoleid
uid=1001, gid=1001
[guest@aaahayan lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unco
nfinet_t:s0-s0:c0.c1023
[guest@aaahayan lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@aaahayan lab5]$  
[guest@aaahayan lab5]$ gedit simoleid2.c  
[guest@aaahayan lab5]$  
[guest@aaahayan lab5]$ gcc simoleid2.c  
[guest@aaahayan lab5]$ gcc simoleid2.c -o simoleid2  
[guest@aaahayan lab5]$ ./simoleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@aaahayan lab5]$ su  
Пароль:  
[root@aaahayan lab5]# chown root:guest simoleid2  
[root@aaahayan lab5]# chmod u+s simoleid2  
[root@aaahayan lab5]# ./simoleid2  
uid=0, gid=0  
[root@aaahayan lab5]# ./simoleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@aaahayan lab5]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-  
s0:c0.c1023  
[root@aaahayan lab5]# chmod g+s simoleid2  
[root@aaahayan lab5]# ./simoleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=0  
[root@aaahayan lab5]# exit  
exit  
[guest@aaahayan lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@aaahayan lab5]$  
[guest@aaahayan lab5]$ gcc readfile.c  
readfile.c: В функции «main»:  
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]  
    while (bytes_read == (buffer));  
                  ^  
[guest@aaahayan lab5]$ gcc readfile.c -o readfile.c  
readfile.c: В функции «main»:  
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]  
    while (bytes_read == (buffer));  
                  ^  
[guest@aaahayan lab5]$ su  
Пароль:  
[root@aaahayan lab5]# chown root:root readfile.c  
[root@aaahayan lab5]# chmod u+s readfile.c  
[root@aaahayan lab5]# chmod -r simoleid.c  
[root@aaahayan lab5]# exit  
exit  
[guest@aaahayan lab5]$ cat simoleid.c  
cat: simoleid.c: Отказано в доступе  
[guest@aaahayan lab5]$ ./readfile.c simoleid.c  
#include <sys/types.h> [guest@aaahayan lab5]$ ./readfile.c /etc/shadow  
root:$6$5wk2oKMw [guest@aaahayan lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
guest2@aaahayan:/tmp
Файл Правка Вид Поиск Терминал Справка
[guest@aaahayan lab5]$ cd /tmp
[guest@aaahayan tmp]$ echo "test" >> file01.txt
[guest@aaahayan tmp]$ cat file01.txt
test
[guest@aaahayan tmp]$ echo "test" > file01.txt
[guest@aaahayan tmp]$ chmod o+rx file01.txt
[guest@aaahayan tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 guest guest 5 окт  6 11:02 file01.txt
[guest@aaahayan tmp]$ su guest2
Пароль:
[guest2@aaahayan tmp]$ cat file01.txt
test
[guest2@aaahayan tmp]$ echo "test" >> file01.txt
[guest2@aaahayan tmp]$ echo "test" > file01.txt
[guest2@aaahayan tmp]$ rm file01.txt
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@aaahayan tmp]$ su
Пароль:
[root@aaahayan tmp]# chmod -t /tmp/
[root@aaahayan tmp]# exit
exit
[guest2@aaahayan tmp]$ rm file01.txt
[guest2@aaahayan tmp]$ su
Пароль:
[root@aaahayan tmp]# chmod +t /tmp/
[root@aaahayan tmp]# exit
exit
[guest2@aaahayan 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.