

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Завен Карапетян

23 сентября, 2024, 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@zkarapetyan ~]$ cd
[guest@zkarapetyan ~]$ mkdir lab5
[guest@zkarapetyan ~]$ cd lab5
[guest@zkarapetyan lab5]$ touch simpleid.c
[guest@zkarapetyan lab5]$ gedit simpleid.c

[guest@zkarapetyan lab5]$
[guest@zkarapetyan lab5]$ gcc simpleid.c
[guest@zkarapetyan lab5]$ gcc simpleid.c -o simpleid
[guest@zkarapetyan lab5]$ ./simpleid
uid=1001, gid=1001
[guest@zkarapetyan lab5]$ id
uid=1001(guest) gid=1001(guest) rpyntu=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_
t:s0-s0:c0.c1023
[guest@zkarapetyan lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@zkarapetyan lab5]$  
[guest@zkarapetyan lab5]$ touch simpleid2.c  
[guest@zkarapetyan lab5]$ gedit simpleid2.c  
[guest@zkarapetyan lab5]$ gcc simpleid2.c  
[guest@zkarapetyan lab5]$ gcc simpleid2.c -o simpleid2  
[guest@zkarapetyan lab5]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@zkarapetyan lab5]$ su  
Пароль:  
[root@zkarapetyan lab5]# chown root:guest simpleid2  
[root@zkarapetyan lab5]# chmod u+s simpleid2  
[root@zkarapetyan lab5]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@zkarapetyan lab5]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@zkarapetyan lab5]# chmod g+s simpleid2  
[root@zkarapetyan lab5]# ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=0  
[root@zkarapetyan lab5]#  
exit  
exit  
[guest@zkarapetyan lab5]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@zkarapetyan lab5]$
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@zkarapetyan lab5]$  
[guest@zkarapetyan lab5]$ touch readfile.c  
[guest@zkarapetyan lab5]$ gedit readfile.c  
[guest@zkarapetyan lab5]$ gcc readfile.c  
readfile.c: В функции «main»:  
readfile.c:20:19: предупреждение: сравнение указателя и целого  
    20 | while (bytes_read == (buffer));  
        |                   ^~  
[guest@zkarapetyan 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@zkarapetyan lab5]$ su  
Пароль:  
[root@zkarapetyan lab5]# v  
bash: v: command not found...  
[root@zkarapetyan lab5]# chown root:root readfile  
[root@zkarapetyan lab5]# chmod -rwx readfile.c  
[root@zkarapetyan lab5]# chmod u+s readfile  
[root@zkarapetyan lab5]# exit  
exit  
[guest@zkarapetyan lab5]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@zkarapetyan lab5]$ ./readfile readfile.c  
#include <stdio.h>[guest@zkarapetyan lab5]$  
[guest@zkarapetyan lab5]$ ./readfile /etc/shadow  
root:$6$0m3pkg1j[guest@zkarapetyan lab5]$  
[guest@zkarapetyan lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@zkarapetyan lab5]$  
[guest@zkarapetyan lab5]$ echo "test" >> /tmp/file01.txt  
[guest@zkarapetyan lab5]$ chmod g+rw /tmp/file01.txt  
[guest@zkarapetyan lab5]$ su guest2  
Пароль:  
su: Сбой при проверке подлинности  
[guest@zkarapetyan lab5]$ su guest2  
Пароль:  
[guest2@zkarapetyan lab5]$ cd /tmp  
[guest2@zkarapetyan tmp]$ cat file01.txt  
test  
[guest2@zkarapetyan tmp]$ echo "test2" >> /tmp/file01.txt  
[guest2@zkarapetyan tmp]$ cat file01.txt  
test  
test2  
[guest2@zkarapetyan tmp]$ echo "test3" > /tmp/file01.txt  
[guest2@zkarapetyan tmp]$ rm file01.txt  
rm: невозможно удалить 'file01.txt': Операция не позволена  
[guest2@zkarapetyan tmp]$ su  
Пароль:  
[root@zkarapetyan tmp]# chmod -t /tmp  
[root@zkarapetyan tmp]#  
exit  
[guest2@zkarapetyan tmp]$ cd /tmp  
[guest2@zkarapetyan tmp]$ echo "test2" >> /tmp/file01.txt  
[guest2@zkarapetyan tmp]$ rm file01.txt  
[guest2@zkarapetyan 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.