Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ким Реачна

5 октябрь, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Теоретическое введение

- 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@kreachna ~]$ mkdir lab5
[guest@kreachna ~]$ cd lab5
[guest@kreachna lab5]$ touch simpleid.c
[guest@kreachna lab5]$
[guest@kreachna lab5]$ gcc simpleid.c -o simpleid
[guest@kreachna lab5]$ ./simpleid
uid=1001, gid=1001
[guest@kreachna lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r
:unconfined_t:s0-s0:c0.c1023
[guest@kreachna lab5]$
```

Рис. 1: результат программы simpleid

Программа simpleid2

```
[guest@kreachna lab5]$ touch simpleid2.c
[guest@kreachna lab5]$ gcc simpleid2.c -o simpleid2
[guest@kreachna lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kreachna lab5]$ su
Password:
[root@kreachna lab5]# chown root:guest /home/guest/simpleid2
chown: cannot access '/home/guest/simpleid2': No such file or directory
[root@kreachna lab5]# chown root:guest simpleid2
[root@kreachna lab5]# chmod u+s simpleid2
[root@kreachna lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@kreachna lab5]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@kreachna lab5]# chmod g+s simpleid2
[root@kreachna lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@kreachna lab5]# exit
exit
```

Рис. 2: результат программы simpleid2

Программа readfile

```
[guest@kreachna lab5]$ touch readfile.c
[guest@kreachna lab5]$ gcc readfile.c
[guest@kreachna lab5]$ gcc readfile.c -o readfile
[guest@kreachna lab5]$ su
Password:
[root@kreachna lab5]# chown root:root readfile
[root@kreachna lab5]# chmod -rwx readfile.c
[root@kreachna lab5]# chmod u+s readfile
[root@kreachna lab5]# exit
exit
[guest@kreachna lab5]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@kreachna lab5]$ ./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;
}
[guest@kreachna lab5]$ ./readfile /etc/shadow
root:$6$QuglvjQbEW.9s2px$LbtOOB0YxGxUpFz1zp3uCcqIYGo6cUW/CNn1cfZex.PI/FzEHLFrIAobtOJh7ZkVKi0BZq0j513l5KzCQ15.X1::0:999
99:7:::
bin:*:19469:0:99999:7:::
daemon:*:19469:0:99999:7:::
adm:*:19469:0:99999:7:::
lp:*:19469:0:99999:7:::
sync:*:19469:0:99999:7:::
shutdown:*:19469:0:99999:7:::
halt:*:19469:0:99999:7:::
mail:*:19469:0:99999:7:::
operator:*:19469:0:99999:7:::
```

Рис. 3: результат программы readfile

Исследование Sticky-бита

```
[guest@kreachna lab5]$ cd /tmp
[guest@kreachna tmp]$ ls -l | grep tmp
drwx------. 2 root root  6 Oct  5 11:42 snap-private-tmp
[guest@kreachna tmp]$ echo "test" >> file01.txt
[guest@kreachna tmp]$ ls -l /file01.txt
ls: cannot access '/file01.txt': No such file or directory
[guest@kreachna tmp]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  5 12:51 /tmp/file01.txt
[guest@kreachna tmp]$ chmod o+rw /tmp/file01.txt
[guest@kreachna tmp]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  5 12:51 /tmp/file01.txt
[guest@kreachna tmp]$ su guest2
Password:
[guest2@kreachna tmp]$ cat /tmp/file01.txt
test
[guest2@kreachna tmp]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@kreachna tmp]$ cat /tmp/file01.txt
test
[guest2@kreachna tmp]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@kreachna tmp]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@kreachna tmp]$ cat /tmp/file01.txt
test
[guest2@kreachna tmp]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[guest2@kreachna tmp]$ su -
Password:
[root@kreachna ~]# chmod -t /tmp
[root@kreachna ~]# exit
logout
[guest2@kreachna tmp]$ ls -l | grep tmp
drwx------. 2 root  root   6 Oct  5 11:42 snap-private-tmp
[guest2@kreachna tmp]$ rm file01.txt
rm: remove write-protected regular file 'file01.txt'?
[guest2@kreachna tmp]$ su -
Password:
[root@kreachna ~]# chmod +t /tmp
[root@kreachna ~]# exit
logout
```

Рис. 4: исследование Sticky-бита

Выводы

Результаты выполнения лабораторной работы

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.