Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Агеева Лада, Нпибд-01-19

3 октября, 2022, Москва, Россия

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@laageeva ~]$ cd dir1
[guest@laageeva dir1]$ touch simpleid.c
[guest@laageeva dir1]$ vi simpleid.c
[guest@laageeva dir1]$ gcc simpleid.c -o simpleid
[guest@laageeva dir1]$ ./simpleid
uid=1001, gid=1001
[guest@laageeva dir1]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023
```

результат программы simpleid

Программа simpleid2

```
[guest@laageeva dir1]$ vi simpleid2.c
[guest@laageeva dir1]$ gcc simpleid2.c -o simpleid2
[guest@laageeva dir1]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@laageeva dir1]$ su
Password:
[root@laageeva dir1]# chown root:guest /home/guest/dir1/simpleid2
[root@laageeva dir1]# chmod u+s /home/guest/dir1/simpleid2
[root@laageeva dir1]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  8 12:22 simpleid2
[root@laageeva dir1]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@laageeva dir1]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s
0-s0:c0.c1023
```

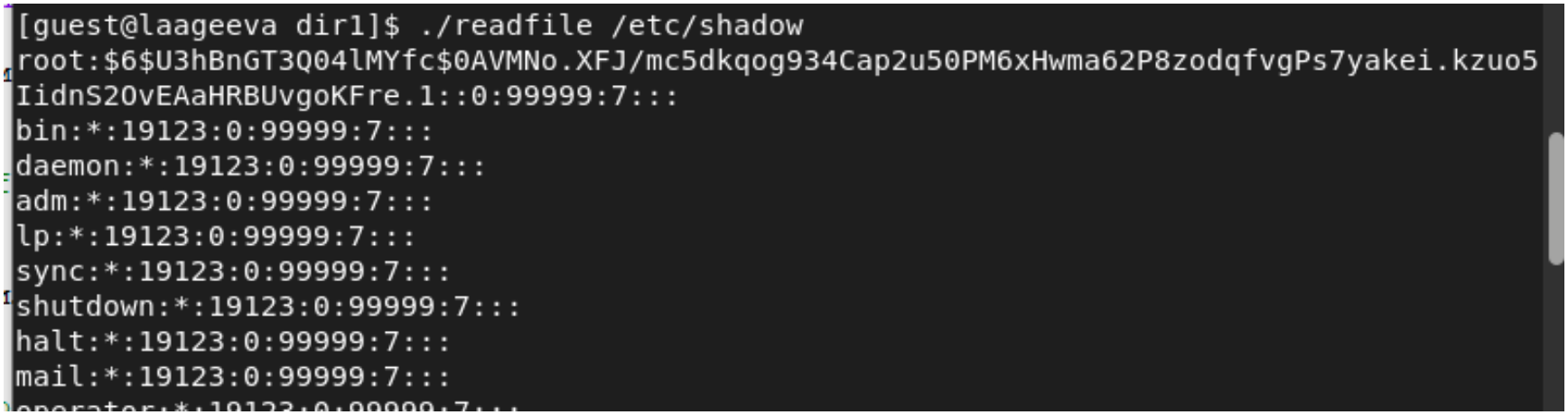
результат программы simpleid2

Программа readfile

```
[root@laageeva dir1]# touch readfile
[root@laageeva dir1]# vi readfile
[root@laageeva dir1]# gcc readfile.c -o readfile
cc1: fatal error: readfile.c: No such file or directory
compilation terminated.
[root@laageeva dir1]# mv readfile readfile.c
[root@laageeva dir1]# gcc readfile.c -o readfile
[root@laageeva dir1]# chown root:root readfile
[root@laageeva dir1]# chmod -r readfile.c
[root@laageeva dir1]# chmod u+s readfile
[root@laageeva dir1]# exit
exit
[guest@laageeva dir1]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@laageeva dir1]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
```

результат программы readfile

Программа readfile



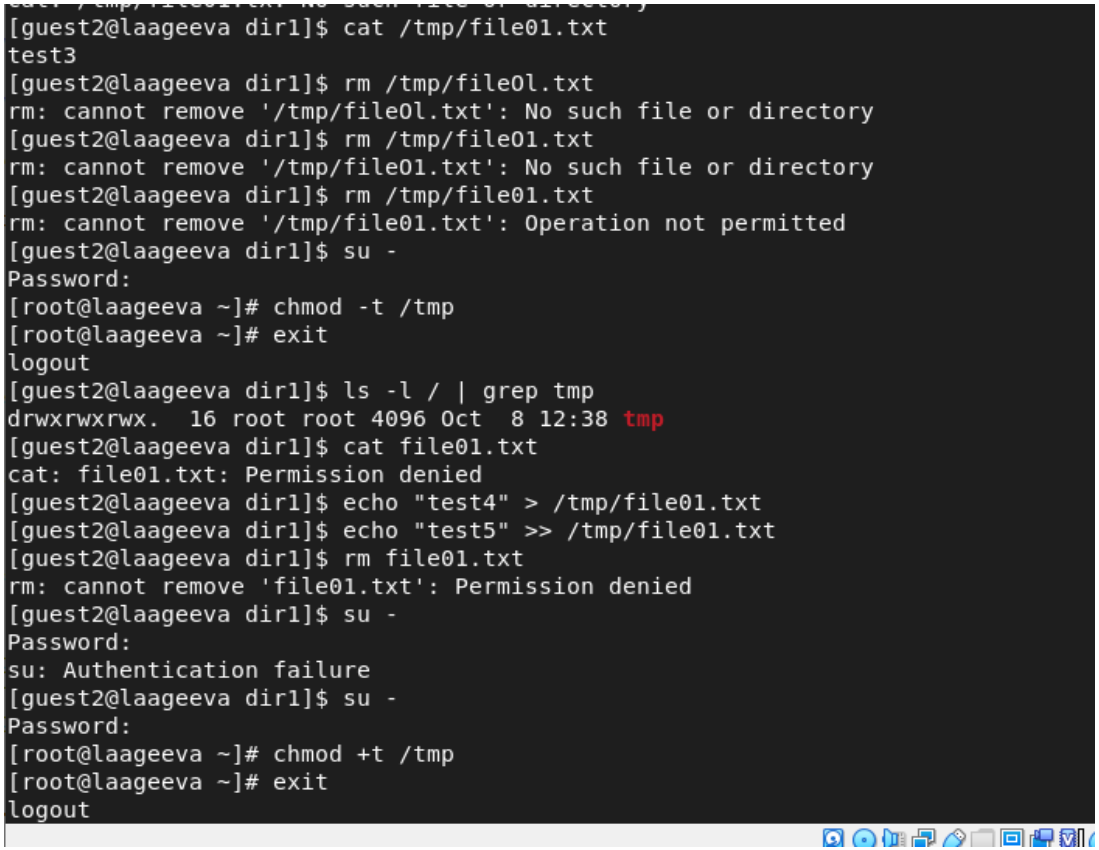
результат программы readfile

Исследование Sticky-бита

```
[guest@laageeva dir1]$ echo "test" > /tmp/file01.txt
[guest@laageeva dir1]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 12:33 /tmp/file01.txt
[guest@laageeva dir1]$ chmod o+rw /tmp/file01.txt
[guest@laageeva dir1]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 12:33 /tmp/file01.txt
[guest@laageeva dir1]$ su gueast2
su: user gueast2 does not exist or the user entry does not contain all the required fie
lds
[guest@laageeva dir1]$ su guest2
Password:
su: Authentication failure
[guest@laageeva dir1]$ su guest2
Password:
su: Authentication failure
[guest@laageeva dir1]$ su guest2
Password:
su: Authentication failure
[guest@laageeva dir1]$ su guest2
Password:
[guest2@laageeva dir1]$ cat /tmp/file01.txt
test
[guest2@laageeva dir1]$ echo "test2" > /tmp/file01.txt
[guest2@laageeva dir1]$ cat /tmp/file01.txt
test2
[guest2@laageeva dir1]$ echo "test3" > /tmp/file01.txt
[guest2@laageeva dir1]$ cat /tmp/file01.tx
cat: /tmp/file01.tx: No such file or directory
[guest2@laageeva dir1]$ cat /tmp/file01.txt
```

исследование Sticky-бита

Исследование Sticky-бита



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.