

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Волков Фрол НПИбд-01-19

8 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

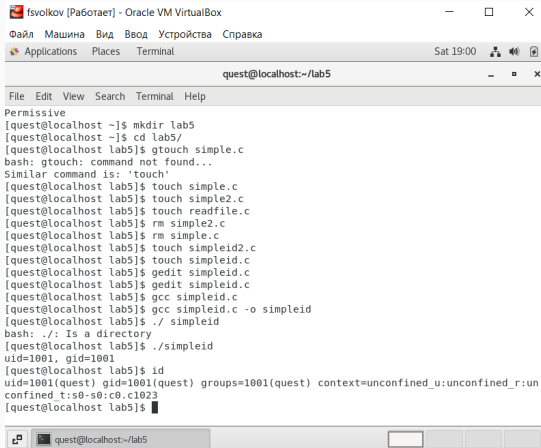
- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться 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

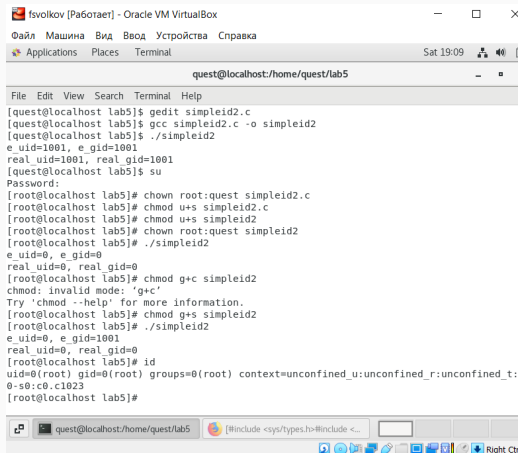
Программа simpleid



```
fsvolkov [Работаer] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places Terminal
Sat 19:00
quest@localhost:~/lab5
File Edit View Search Terminal Help
Permissive
[quest@localhost ~]$ mkdir lab5
[quest@localhost ~]$ cd lab5/
[quest@localhost lab5]$ gtouch simple.c
bash: gtouch: command not found...
Similar command is: 'touch'
[quest@localhost lab5]$ touch simple.c
[quest@localhost lab5]$ touch simple2.c
[quest@localhost lab5]$ touch readfile.c
[quest@localhost lab5]$ rm simple2.c
[quest@localhost lab5]$ rm simple.c
[quest@localhost lab5]$ touch simpleid2.c
[quest@localhost lab5]$ touch simpleid.c
[quest@localhost lab5]$ gedit simpleid.c
[quest@localhost lab5]$ gedit simpleid.c
[quest@localhost lab5]$ gcc simpleid.c
[quest@localhost lab5]$ gcc simpleid.c -o simpleid
[quest@localhost lab5]$ ./ simpleid
bash: ./: Is a directory
[quest@localhost lab5]$ ./simpleid
uid=1001, gid=1001
[quest@localhost lab5]$ id
uid=1001(quest) gid=1001(quest) groups=1001(quest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[quest@localhost lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

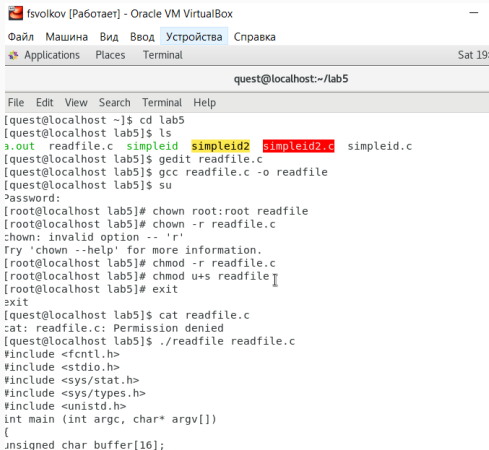


```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places Terminal Sat 19:09
quest@localhost:/home/quest/lab5

File Edit View Search Terminal Help
[quest@localhost lab5]$ gedit simpleid2.c
[quest@localhost lab5]$ gcc simpleid2.c -o simpleid2
[quest@localhost lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real uid=1001, real gid=1001
[quest@localhost lab5]$ su
Password:
[root@localhost lab5]# chown root:quest simpleid2.c
[root@localhost lab5]# chmod u+s simpleid2.c
[root@localhost lab5]# chown root:quest simpleid2
[root@localhost lab5]# ./simpleid2
e_uid=0, e_gid=0
real uid=0, real gid=0
[root@localhost lab5]# chmod g+c simpleid2
chmod: invalid mode: 'g+c'
Try 'chmod --help' for more information.
[root@localhost lab5]# chmod g+s simpleid2
[root@localhost lab5]# ./simpleid2
e_uid=0, e_gid=1001
real uid=0, real gid=0
[root@localhost lab5]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:
0-s0:c0.c1023
[root@localhost lab5]#
```

Figure 2: результат программы simpleid2

Программа readfile



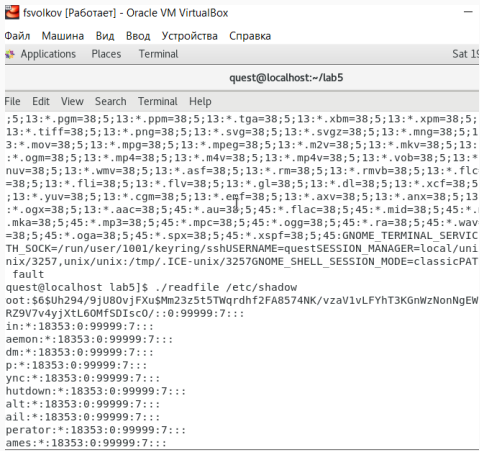
```
fsvolkov [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  Sat 19:

quest@localhost:~/lab5

File  Edit  View  Search  Terminal  Help
[quest@localhost ~]$ cd lab5
[quest@localhost lab5]$ ls
a.out  readfile.c  simpleid  simpleid2  simpleid2.c  simpleid.c
[quest@localhost lab5]$ gedit readfile.c
[quest@localhost lab5]$ gcc readfile.c -o readfile
[quest@localhost lab5]$ su
Password:
[root@localhost lab5]# chown root:root readfile
[root@localhost lab5]# chown -r readfile.c
chown: invalid option -- 'r'
Try 'chown --help' for more information.
[root@localhost lab5]# chmod -r readfile.c
[root@localhost lab5]# chmod u+s readfile.c
[root@localhost lab5]# exit
exit
[quest@localhost lab5]$ cat readfile.c
cat: readfile.c: Permission denied
[quest@localhost 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];
```

Figure 3: результат программы readfile

Программа readfile



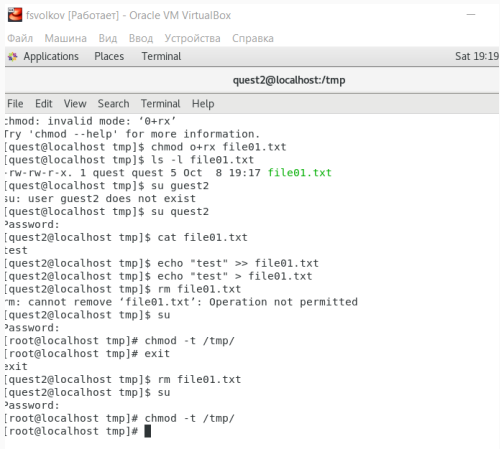
```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
quest@localhost:~/lab5

File Edit View Search Terminal Help

;5;13:*.pgm=38;5;13:*.ppm=38;5;13:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;
13:*.tiff=38;5;13:*.png=38;5;13:*.svg=38;5;13:*.svgz=38;5;13:*.mng=38;5;1
3:*.mov=38;5;13:*.mpg=38;5;13:*.mpeg=38;5;13:*.m2v=38;5;13:*.mkv=38;5;13:
:*.ogm=38;5;13:*.mp4=38;5;13:*.m4v=38;5;13:*.mp4v=38;5;13:*.vob=38;5;13:*.
nuv=38;5;13:*.wmv=38;5;13:*.asf=38;5;13:*.rm=38;5;13:*.rmvb=38;5;13:*.flc
=38;5;13:*.fli=38;5;13:*.flv=38;5;13:*.gl=38;5;13:*.dl=38;5;13:*.xcf=38;5
;13:*.yuv=38;5;13:*.cgm=38;5;13:*.epf=38;5;13:*.axv=38;5;13:*.anx=38;5;13
:*.ogx=38;5;13:*.aac=38;5;45:*.au=38;5;45:*.flac=38;5;45:*.mid=38;5;45:*.
.mka=38;5;45:*.mp3=38;5;45:*.mpc=38;5;45:*.ogg=38;5;45:*.ra=38;5;45:*.wav
=38;5;45:*.oga=38;5;45:*.spx=38;5;45:*.xspf=38;5;45:GNOME_TERMINAL_SERVIC
TH_SOCKET/run/user/1001/keyring/sshUSERNAME=quest$SESSION_MANAGER=local/uni
nix/3257,unix/unix:/tmp/.ICE-unix/3257GNOME_SHELL_SESSION_MODE=classicPAT
fault
quest@localhost lab5]$ ./readfile /etc/shadow
oot:$6$Uh294/9jU80vjFXu$Mm23z5t5TWqrdf2FA8574NK/vzaV1vLFyHt3K6nWzNonNgEW
RZ9V7v4yjtL60MfSDIsc0/:0:99999:7:::
in:*.18353:0:99999:7:::
aemon:*.18353:0:99999:7:::
dm:*.18353:0:99999:7:::
p:*.18353:0:99999:7:::
ync:*.18353:0:99999:7:::
hutdown:*.18353:0:99999:7:::
alt:*.18353:0:99999:7:::
ail:*.18353:0:99999:7:::
perator:*.18353:0:99999:7:::
ames:*.18353:0:99999:7:::
```

Figure 4: результат программы readfile

Исследование Sticky-бита



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
Sat 19:19

quest2@localhost:/tmp

File Edit View Search Terminal Help
chmod: invalid mode: '0+rx'
Try 'chmod --help' for more information.
[quest2@localhost tmp]$ chmod o+rx file01.txt
[quest2@localhost tmp]$ ls -l file01.txt
-rw-rw-r-x. 1 quest quest 5 Oct  8 19:17 file01.txt
[quest2@localhost tmp]$ su guest2
su: user guest2 does not exist
[quest2@localhost tmp]$ su guest2
password:
[quest2@localhost tmp]$ cat file01.txt
test
[quest2@localhost tmp]$ echo "test" >> file01.txt
[quest2@localhost tmp]$ echo "test" > file01.txt
[quest2@localhost tmp]$ rm file01.txt
rm: cannot remove 'file01.txt': Operation not permitted
[quest2@localhost tmp]$ su
password:
[root@localhost tmp]# chmod -t /tmp/
[root@localhost tmp]# exit
exit
[quest2@localhost tmp]$ rm file01.txt
[quest2@localhost tmp]$ su
password:
[root@localhost tmp]# chmod -t /tmp/
[root@localhost tmp]#
```

Figure 5: 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.