

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Пименов Михаил НБИ-01-19

3 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

```
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ cd  
[guest@mppimenov ~]$ mkdir lab5  
[guest@mppimenov ~]$ touch simpleid.c  
[guest@mppimenov ~]$ touch simpleid2.c  
[guest@mppimenov ~]$ touch readfile.c  
[guest@mppimenov ~]$ mv simpleid.c simpleid2.c readfile.c lab5/  
[guest@mppimenov ~]$ cd lab5/  
[guest@mppimenov lab5]$ gedit simpleid.c  
[guest@mppimenov lab5]$ gcc simpleid.c  
[guest@mppimenov lab5]$ gcc simpleid.c -o simpleid  
[guest@mppimenov lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@mppimenov lab5]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@mppimenov lab5]$
```

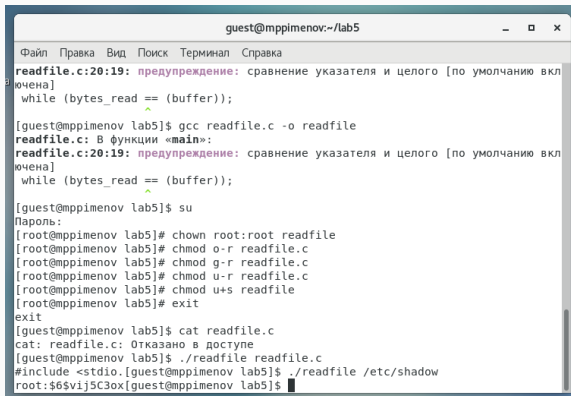
Figure 1: результат программы simpleid

Программа simpleid2

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

Figure 2: результат программы simpleid2

Программа readfile



```
guest@mppimenov:~/lab5
Файл  Правка  Вид  Поиск  Терминал  Справка
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию вкл
ючена]
while (bytes_read == (buffer));
^
[guest@mppimenov lab5]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию вкл
ючена]
while (bytes_read == (buffer));
^
[guest@mppimenov lab5]$ su
Пароль:
[root@mppimenov lab5]# chown root:root readfile
[root@mppimenov lab5]# chmod o-r readfile.c
[root@mppimenov lab5]# chmod g-r readfile.c
[root@mppimenov lab5]# chmod u-r readfile.c
[root@mppimenov lab5]# chmod u+s readfile
[root@mppimenov lab5]# exit
exit
[guest@mppimenov lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@mppimenov lab5]$ ./readfile readfile.c
#include <stdio.h>[guest@mppimenov lab5]$ ./readfile /etc/shadow
root:$6$vi5C3ox[guest@mppimenov lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
guest2@mppimenov:tmp
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@mppimenov tmp]$ ls -l /tmp/file01.txt
-rw-rwxr-x. 1 guest guest 5 окт  3 17:07 /tmp/file01.txt
[guest@mppimenov tmp]$ chmod g=rx file01.txt
[guest@mppimenov tmp]$ ls -l /tmp/file01.txt
-rw-r-xr-x. 1 guest guest 5 окт  3 17:07 /tmp/file01.txt
[guest@mppimenov tmp]$ su guest2
Пароль:
[guest2@mppimenov tmp]$ cat file01.txt
test
[guest2@mppimenov tmp]$ echo "test" >> file01.txt
bash: file01.txt: Отказано в доступе
[guest2@mppimenov tmp]$ echo "test" > file01.txt
bash: file01.txt: Отказано в доступе
[guest2@mppimenov tmp]$ crm file01.txt
bash: crm: команда не найдена...
[guest2@mppimenov tmp]$ rm file01.txt
rm: удалить защищенный от записи обычный файл «file01.txt»? y
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest2@mppimenov tmp]$ su
Пароль:
[root@mppimenov tmp]# chmod -t /tmp/
[root@mppimenov tmp]# exit
exit
[guest2@mppimenov tmp]$ echo "test" >> file01.txt
bash: file01.txt: Отказано в доступе
[guest2@mppimenov tmp]$ echo "test" > file01.txt
bash: file01.txt: Отказано в доступе
[guest2@mppimenov tmp]$ rm file01.txt
rm: удалить защищенный от записи обычный файл «file01.txt»? y
[guest2@mppimenov tmp]$ su
Пароль:
[root@mppimenov tmp]# chmod +t /tmp/
[root@mppimenov 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.