Лабораторная работа №5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Захарова Софья Михайловна

Цель 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.

> Зада-

ние

Лабораторная paбота подpaзумевает paботу \mathbf{c} виртуальной машиной Virtual Box,опеpaционной системой Linux, дистрибути-BOMCentos и закрепление теоpeтических ocнов полу₂ чения

практических на-

Выполнение лабораторной работы

1. Вошла в систему от имени пользователя guest. (рис.1).

[guest@smzakharoval ~]\$

Рис. 1: Рис.1. Вход в систему.

2. Создала программу simpleid.c. (рис.2).

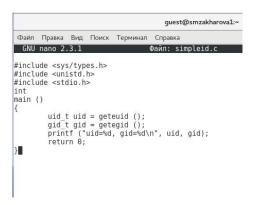


Рис. 2: Рис.2. Создание программы.

3. Скомпилировала программу и убедилась, что файл программы создан (рис.3).

```
[guest@smzakharoval ~]$ nano simpleid.c
[guest@smzakharoval ~]$ gcc simpleid.c -o simpleid
[guest@smzakharoval ~]$ ■
```

Рис. 3: Рис.3. Компиляция файла.

4. Выполнила программу simpleid: ./simpleid (рис.4):

```
[guest@smzakharoval ~]$ ./simpleid
uid=1001, gid=1001
[guest@smzakharoval ~]$ ■
```

Рис. 4: Рис.4. Выполнение программы.

5. Выполнила системную программу id и сравнила полученный результат с данными предыдущего пункта задания: программа работает верно, результаты совпадают. (рис.5):

```
[guest8smaxkharoval -]s id uid-1001[guest) gid-1001[guest] xohrexcr=unconfined_u:unconfined_r:u longfined_t:s0-s0:0.e1023 [guesteszakharoval -]s 

[guest8smaxkharoval -]s
```

Рис. 5: Рис.5. Выполнение программы и сравнение с предыдущей.

6. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c (рис. 6).

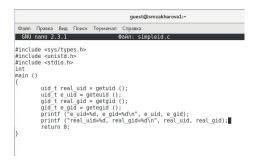


Рис. 6: Рис.6. Усложнение программы.

- 7. Скомпилировала и запустила simpleid2.c (рис.7).
- 8. От имени суперпользователя выполнила команды: chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2 C помощью этих команд файлу simpleid2 изменила владельца и группу на root и guest соответственно, а также установила на файл SetUID-бит. (рис. 8).

```
[guest@smzakharoval ~]$ gcc simpleid2.c -o simpleid2
[guest@smzakharoval ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@smzakharoval ~]$ [
```

Рис. 7: Рис.7. Компиляция и запуск второй программы.

Рис. 8: Рис.8. Выполнение команд.

9. Временно повысила свои права с помощью команды su (рис. 9).

Рис. 9: Рис.9. Повышение прав.

- 10. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls —l simpleid2 (рис. 10).

 11. Запустила simpleid2 и id. Результаты совпадают. (рис.11)

 12. Проделала тоже самое относительно SetGID-бита (рис.12).

 13. Создала программу readfile.c (рис.13).

 14. Откомпилировала её (рис.14).
- 15. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог (puc.15).

```
[root@smzakharoval guest]# ls -l simpleid2
-гиягихг-х. l root guest 8656 ноя 12 16:16 <mark>simpleid2</mark>
[root@smzakharoval guest]# |
```

Рис. 10: Рис.10. Проверка.

```
[root@smzakharoval guest]# ./simpleid2
e_uid=0, e_gld=0
real_uid=0, real_gld=0
[root@smzakharoval guest]# id
uid=@root_gld=0[root]# root_gld=0
uid=@root_gld=(root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld=0root_gld
```

Рис. 11: Рис.11. Запуск команд.

```
|Tool@anzakharoval guest|# choom root:guest /home/guest/simple1d2
|Tool@anzakharoval guest|# chood us- /home/guest/simple1d2
|Tool@anzakharoval guest|# chood us- /home/guest/simple1d2
|Tool@anzakharoval guest|# is -l. simple1d2
|Tool@anzakharoval guest|# is -l. simple1d3
|Solego (cl.Cl23
|Tool@anzakharoval guest|# is -l. simple1d3
|Tool@anzakharoval guest|# is -l. simple1d4
```

Рис. 12: Рис.12. Запуск команд.

```
guest@smrzakharowiI/home/guest

dwan Tpaska Bun Toxick Tepowskan Crpaska

GNU nano 2.3.1

ONTH: readfile.C

Ginclude <frid.h>
#include <sys/fytes.h>
#include <sys/fytes.h

#include <sys/fytes.h>
#include <sys/fytes.h>
#include <sys/fytes.h

#include <s
```

Рис. 13: Рис.13. Запуск команд.

```
[root@smzakharoval guest]# gcc readfile.c -o readfile
[root@smzakharoval guest]# █
```

Рис. 14: Рис.14. Компиляция.

```
[root@smzakharoval guest]# chmod 000 readfile.c
[root@smzakharoval guest]# ■
```

Рис. 15: Рис.15. Изменение прав.

16. Проверила, что пользователь guest не может прочитать файл readfile.c (рис.16).

```
[root@smzakharoval guest]# su guest
[guest@smzakharoval ~]$ gcc readfile.c -o readfile
ccl: фатальная ошибка: readfile.c: Отказано в доступе
компиляция прервана.
[guest@smzakharoval ~]$
```

Рис. 16: Рис.16. Проверка.

17. Сменила у программы readfile владельца и установила SetU'D-бит (рис.17).

```
[root@smzakharoval guest]# chmod 777 readfile.c
[root@smzakharoval guest]# chmod +s readfile.c
[root@smzakharoval guest]#
```

Рис. 17: Рис.17. Изменение прав.

18. Проверила, может ли программа readfile прочитать файл readfile.c (рис.18).



Рис. 18: Рис.18. Проверка.

- 19. Проверила, может ли программа readfile прочитать файл /etc/shadow. Может (рис.19).
- 20. Исследование Sticky-бита

Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ls -l / | grep tmp (рис.20).



Рис. 19: Рис.19. Проверка.

```
[guest@smzakharovāl ~]$ ls -l / | grep tmp
drwxrwxrwt. 24 root root 4096 ноя 12 16:35 <mark>tmp</mark>
[guest@smzakharoval ~]$ ∏
```

Рис. 20: Рис.20. Проверка наличия атрибута.

21. От имени пользователя guest создала файл file 01.txt в директории /tmp со словом test: echo "test" > /tmp/file 01.txt (puc.21).

> |[guest@smzakharoval ~]\$ echo "test" > /tmp/file01.txt |[guest@smzakharoval ~]\$ **|**

Рис. 21: Рис.21. Создание файла.

- 22. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные». Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме «остальных пользователей» (рис.22).
- 23. От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt (рис.23).
- 24. От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2, стерев при этом всю имеющуюся в файле информацию с помощью команды echo "test2" > /tmp/file01.txt. Выполнить операцию удалось (рис.24).
- 25. Проверила содержимое файла командой са
t $/{\rm tmp/file01.txt}$ (рис.25).
- 26. От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt

```
iguest@smzakharoval -j$ ls -l /tmp/file01.txt
-гм-гм-г-. 1 guest guest 5 ноя 12 16:39 /tmp/file01.txt
[guest@smzakharoval -]$ chmod o+гм /tmp/file01.txt
[guest@smzakharoval -]$ ls -l /tmp/file01.txt
-гм-гм-гм-. 1 guest guest 5 ноя 12 16:39 /tmp/file01.txt
[guest@smzakharoval -]$
```

Рис. 22: Рис.22. Проверка атрибута и изменение прав.

[root@smzakharoval guest]# su guest2 [guest2@smzakharoval guest]\$ cat /tmp/file01.txt test [guest2@smzakharoval guest]\$ ■

Рис. 23: Рис.23. Попытка чтения.

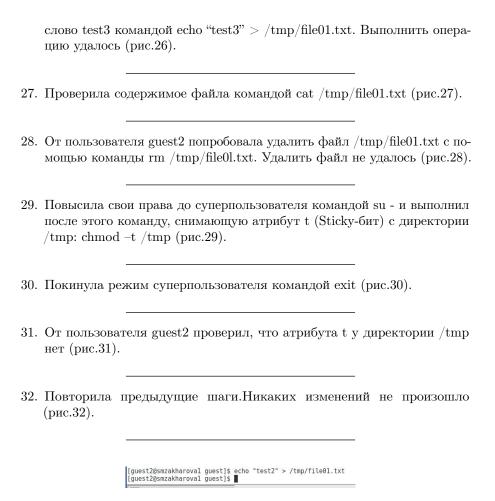


Рис. 24: Рис.24. Изменение информации в файле.

```
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
test2
[guest2@smzakharoval guest]$ ■
```

Рис. 25: Рис.25. Проверка содержимого.

```
[guest2@smzakharova1 guest]$ echo "test3" > /tmp/file01.txt
[guest2@smzakharova1 guest]$ █
```

Рис. 26: Рис.26. Изменение информации в файле.

```
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharoval guest]$ ■
```

Рис. 27: Рис.27. Проверка содержимого.

```
[guest2@smzakharoval guest]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Операция не позволена
[guest2@smzakharoval guest]$ [
```

Рис. 28: Рис.28. Попытка удаления.

```
[guest2@smzakharoval guest]$ su
Пароль:
[root@smzakharoval guest]# chmod -t /tmp
[root@smzakharoval guest]# ■
```

Рис. 29: Рис.29. Повышение прав и снятие атрибута.

```
[root@smzakharoval guest]# exit
exit
[guest2@smzakharoval guest]$
```

Рис. 30: Рис.30. Выход из режима суперпользователя.

```
[guest2@smzakharoval guest]$ ls -l / | grep tmp
drwxrwxrwx. 24 root root 4096 ноя 12 16:39 tmp
[guest2@smzakharoval guest]$ ▮
```

Рис. 31: Рис.31. Проверка на наличие атрибута.

```
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharoval guest]$ echo "test2" > /tmp/file01.txt
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
test2
[guest2@smzakharoval guest]$ echo "test3" > /tmp/file01.txt
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
test3
[guest2@smzakharoval guest]$ cat /tmp/file01.txt
[guest2@smzakharoval guest]$
```

Рис. 32: Рис.32. Дублирование предыдущих шагов.

33. Проверила, удалось ли удалить файл от имени пользователя, не являющегося его владельцем? Удалось (рис.33).

[guest2@smzakharoval guest]\$ rm /tmp/file01.txt [guest2@smzakharoval guest]\$ ■

Рис. 33: Рис.33. Проверка удаления.

34. Повысила свои права до суперпользователя с помощью команды su - и вернула атрибут t на директорию /tmp (puc.34).

[guest2@smzakharoval guest]\$ su Пароль: [root@smzakharoval guest]# chmod +t /tmp [root@smzakharoval guest]# exit exit [guest2@smzakharoval guest]\$ ■

Рис. 34: Рис.34. Установка атрибута.

D. .

Вы-

во-

ды

Благодаря данной ла-

бо-

pa-

торной

pa-

бо-

те, я изу-

чил

ме-

xa-

низ-

мы из-

ме-

не-

ния иден-

ти-

фи-

ка-

TO-

ров,

при-

ме-

не-

ния

SetUID-

И

Sticky-

битов.

По-

лу-

чил

прак-

ти-

че-

ские

на-

вы-

ки

pa-

бо 12 ты в

кон-

соли

с допол-

ни-

тель-

Спасибо за внимание!