Лабораторная работа 5

Поляков Арсений Андреевич, НФИбд-01-19

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Поляков Арсений Андреевич

Группа: НФИбд-01-19

МОСКВА

2022 г.

Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов.

Выполнение лабораторной работы

1. Создал программу simpleid.c.

```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t uid = geteuid ();
gid_t gid = getegid ();
printf ("uid=%d, gid=%d\n", uid, gid);
return 0;
}
```

simpleid

2. Скомпилировал и выполнил программу. Сравнил с id. Как видим, результат работы команд - одинаковый.

```
[guest@a Lab5]$ gcc simpleid.c -o simpleid
[guest@a Lab5]$ ./simpleid
uid=1001, gid=1001
[guest@a Lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

compile and run

3. Усложнил программу, добавив вывод действительных идентификаторов.

```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t real_uid = getuid ();
uid_t e_uid = geteuid ();
gid_t real_gid = getgid ();
gid_t e_gid = getegid () ;
printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
printf ("real_uid=%d, real_gid=%d\n", real_uid,real_gid);
return 0;
}
```

simpleid2.c

4. Скомпилировал и запустил simpleid2.c.

```
[guest@a Lab5]$ gcc simpleid2.c -o simpleid2
[guest@a Lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

simpleid2

5. От имени суперпользователя выполнил команды

```
[root@a ~]# chown root:guest /home/guest/Lab5/simpleid2
[root@a ~]# chmod u+s /home/guest/Lab5/simpleid2
```

chmod

6. Запустил simpleid2 и id

```
[guest@a Lab5]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  8 15:01 simpleid2
[guest@a Lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
```

simpleid2 run

7. Создал программу readfile.c:

```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;
}
```

readfile.c

8. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.

```
[root@a ~]# chown root:guest /home/guest/Lab5/readfile.c
[root@a ~]# chmod 700 /home/guest/Lab5/readfile.c
```

chown

9. guest не может прочитать файл readfile.c

Can`t read

10. Сменил у программы readfile владельца и установил SetU'D-бит

```
[root@a ~]# chown guest:guest /home/guest/Lab5/readfile.c
[root@a ~]# chmod u+s /home/guest/Lab5/readfile.c
```

readfile

11. Проверил прочитать файл readfile и /etc/shadow

```
[guest@a Lab5]$ ./readfile readfile
```

readfile read

```
[guest@a Lab5]$ ./readfile /etc/shadow
```

/etc/shadow read

12. readfile удалось прочитать, а /etc/shadow - нет

13. Проверил sticky бит на категории tmp. Создал файл в tmp от guest и посмотерл атрибуты.

```
[guest@a ~]$ ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 Oct  8 15:14 tmp
[guest@a ~]$ echo "test" > /tmp/file01.txt
[guest@a ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 15:17 /tmp/file01.txt
[guest@a ~]$ chmod o+rw /tmp/file01.txt
[guest@a ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 15:17 /tmp/file01.txt
```

sticky

14. От guest2 попробовал выполнить различные операции

```
[guest@a ~]$ su - guest2
Password:
[guest2@a ~]$ cat /tmp/file01.txt
test
[guest2@a ~]$ echo "test2" > /tmp/file01.txt
[guest2@a ~]$ cat /tmp/file01.txt
test2
[guest2@a ~]$ echo "test2" >> /tmp/file01.txt
[guest2@a ~]$ cat /tmp/file01.txt
test2
test2
[guest2@a ~]$ echo "test3" > /tmp/file01.txt
[guest2@a ~]$ cat /tmp/file01.txt
test3
[guest2@a ~]$ rm /tmp/fileOl.txt
rm: cannot remove '/tmp/fileOl.txt': No such file or directory
```

guest2 file01

15. Не удалось выполнить только rm

16. Снял атрибут t (Sticky-бит) сдиректории /tmp

```
[root@a ~]# chmod -t /tmp
```

-t

17. Повторил предыдущие шаги. Изменений нет

```
[guest2@a ~]$ ls -l / | grep tmp
drwxrwxrwx.  16 root root 4096 Oct  8 15:19 tmp
[guest2@a ~]$ echo "test2" >> /tmp/file01.txt
[guest2@a ~]$ cat /tmp/file01.txt
test3
test2
[guest2@a ~]$ echo "test2" >> /tmp/file01.txt
[guest2@a ~]$ cat /tmp/file01.txt
test3
test2
test2
[guest2@a ~]$ echo "test2" > /tmp/file01.txt
[guest2@a ~]$ rm /tmp/fileOl.txt
rm: cannot remove '/tmp/fileOl.txt': No such file or directory
```

guest2 file01 try 2

Вывод

Выполнив данную лабораторную работу, я получение практические навыков работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

1. Кулябов, Д.С. - Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов https://esystem.rudn.ru/pluginfile.php/1651889/mod_resource/content/2/005-lab_discret_sticky.pdf