

Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Павличенко Родион Андреевич

Российский университет дружбы народов

1 1. Информация

2 2. Выполнение лабораторной работы

Раздел 1

1. Информация

1.1 Докладчик

- **ФИО:** Павличенко Родион Андреевич
- **Статус:** Студент
- **Группа:** НПИбд-02-24
- **ВУЗ:** Российский университет дружбы народов
им. П. Лумумбы
- **Почта:** 1132246838@pfur.ru

Раздел 2

2. Выполнение лабораторной работы

2.1 Вошли в систему от имени пользователя guest. Создали программу simpleid.c

```
[rapavlichenko@rapavlichenko ~]$ su guest
Password:
[guest@rapavlichenko rapavlichenko]$ touch simpleid.c
touch: cannot touch 'simpleid.c': Permission denied
[guest@rapavlichenko rapavlichenko]$ cd ~
[guest@rapavlichenko ~]$ touch simpleid.c
[guest@rapavlichenko ~]$ nano simplified.c
[guest@rapavlichenko ~]$
```

2.2 Скомпилировали программу и убедились, что файл программы создан. Выполнили программу simpleid. Выполнили системную программу id

```
[guest@rapavlichenko ~]$ gcc simpleid.c -o simpleid
[guest@rapavlichenko ~]$ ./ simpleid
bash: ./: Is a directory
[guest@rapavlichenko ~]$ ./simpleid
uid=1001, gid=1001
[guest@rapavlichenko ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@rapavlichenko ~]$
```

2.3 Усложнили программу, добавив вывод действительных идентификаторо

```
[guest@rapavlichenko ~]$ touch simpleid2.c  
[guest@rapavlichenko ~]$ nano s[im]pleid2.c  
[guest@rapavlichenko ~]$
```


2.4 Скомпилировали и запустили simpleid2.c

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

2.5 От имени суперпользователя выполнили команды:
chown root:guest /home/guest/simpleid2; chmod u+s
/home/guest/simpleid

```
[rapavlichenko@rapavlichenko ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] password for rapavlichenko:
[rapavlichenko@rapavlichenko ~]$ sudo chmod u+s /home/guest/simpleid2
[rapavlichenko@rapavlichenko ~]$
```

2.6 Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустили simpleid2 и id

```
[guest@rapavlichenko ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 17656 Feb 22 08:47 simpleid2
[guest@rapavlichenko ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@rapavlichenko ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unco
nfinned_r:unconfined_t:s0-s0:c0.c1023
[guest@rapavlichenko ~]$
```

2.7 Проделали тоже самое относительно SetGID-бита

```
[guest@rapavlichenko ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@rapavlichenko ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unco
nfinied_r:unconfined_t:s0-s0:c0.c1023
[guest@rapavlichenko ~]$
```

2.8 Создали программу readfile.c и откомпилировали ее

```
[guest@rapavlichenko ~]$ touch readfile.c  
[guest@rapavlichenko ~]$ nano readfile.c  
[guest@rapavlichenko ~]$ gcc readfile.c -o readfile  
[guest@rapavlichenko ~]$
```

2.9 Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог

```
[rapavlichenko@rapavlichenko ~]$ sudo chown root:root /home/guest/readfile.c
[rapavlichenko@rapavlichenko ~]$ sudo chmod 660 /home/guest/simpleid2
[rapavlichenko@rapavlichenko ~]$ sudo chmod 660 /home/guest/readfile.c
[rapavlichenko@rapavlichenko ~]$
```

2.10 Проверили, что пользователь `guest` не может прочитать файл `readfile.c`.

```
[ Error reading readfile.c: Permission denied ]
```

^O Write Out	^W Where Is	^K Cut	^T Execu
^R Read File	^\ Replace	^U Paste	^J Justi

2.11 Сменили у программы readfile владельца и установили SetU'D-бит

```
[rapavlichenko@rapavlichenko ~]$ sudo chown root:root /home/guest/readfile
[sudo] password for rapavlichenko:
[rapavlichenko@rapavlichenko ~]$ sudo chmod u+s /home/guest/readfile
[rapavlichenko@rapavlichenko ~]$
```


2.12 Проверили, может ли программа readfile прочитать файл readfile.c. Она может

```
[guest@rapavlichenko ~]$ ./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];
    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]);
    }
```

2.13 Проверили, может ли программа readfile прочитать файл /etc/shadow. Она может

```
[guest@rapavlichenko ~]$ ./readfile /etc/shadow
root:$6$2DGS3DzNxjz4v3Ef$vb.9EXKNiZz2MHIQafBCOXh0HALYzBTpWyg1bbk1AhdtZwHd7
4gHHibEL8Rqn0EBN6mAk6/UXcvhX6.Ahge0::0:99999:7:::
bin:*:19820:0:99999:7:::
daemon:*:19820:0:99999:7:::
adm:*:19820:0:99999:7:::
lp:*:19820:0:99999:7:::
sync:*:19820:0:99999:7:::
shutdown:*:19820:0:99999:7:::
halt:*:19820:0:99999:7:::
mail:*:19820:0:99999:7:::
operator:*:19820:0:99999:7:::
games:*:19820:0:99999:7:::
```

2.14 Выяснили, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду `ls -l / | grep tmp`. От имени пользователя `guest` создали файл `file01.txt` в директории `/tmp` со словом `test`. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»

```
[guest@rapavlichenko ~]$ ls -l / | grep tmp
drwxrwxrwt. 23 root root 4096 Feb 22 09:09 tmp
[guest@rapavlichenko ~]$ echo "test" > /tmp/file01.txt
[guest@rapavlichenko ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Feb 22 09:13 /tmp/file01.txt
[guest@rapavlichenko ~]$ chmod o+rw /tmp/file01.txt
[guest@rapavlichenko ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Feb 22 09:13 /tmp/file01.txt
[guest@rapavlichenko ~]$
```

2.15 От пользователя guest2 попробуйте прочитать файл /tmp/file01.txt. От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2. Операцию выполнить не удалось. Проверили содержимое файла командой cat /tmp/file01.txt. От пользователя guest2 попробовали записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию. Выполнить операцию не удалось. Проверили содержимое файла командой cat /tmp/file01.txt

```
[rapavlichenko@rapavlichenko ~]$ su guest2
Password:
su: Authentication failure
[rapavlichenko@rapavlichenko ~]$ su guest2
Password:
[guest2@rapavlichenko rapavlichenko]$ cat /tmp/file01.txt
test
```

2.16 От пользователя guest2 попробовали удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt`. Не удалось удалить файл.

```
[guest2@rapavlichenko rapavlichenko]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@rapavlichenko rapavlichenko]$ ,.
```

2.17 Повысили свои права до суперпользователя и выполнили после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`. Покинули режим суперпользователя командой `exit`. От пользователя `guest2` проверили, что атрибута `t` у директории `/tmp` нет

```
[guest2@rapavlichenko rapavlichenko]$ su -  
Password:  
[root@rapavlichenko ~]# chmod -t /tmp  
[root@rapavlichenko ~]# exit  
logout  
[guest2@rapavlichenko rapavlichenko]$ s -l / | grep tmp  
bash: s: command not found...  
[guest2@rapavlichenko rapavlichenko]$ ls -l / | grep tmp  
drwxrwxrwx. 23 root root 4096 Feb 22 09:22 tmp  
[guest2@rapavlichenko rapavlichenko]$
```

2.18 Повторили предыдущие шаги. Все действия, кроме удаления выполнить не удалось.

```
[guest2@rapavlichenko rapavlichenko]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@rapavlichenko rapavlichenko]$ cat /tmp/file01.txt
test
[guest2@rapavlichenko rapavlichenko]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@rapavlichenko rapavlichenko]$ cat /tmp/file01.txt
test
[guest2@rapavlichenko rapavlichenko]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@rapavlichenko rapavlichenko]$
```

2.19 Повысили свои права до суперпользователя и вернули атрибут `t` на директорию `/tmp`

```
[guest2@rapavlichenko rapavlichenko]$ su -  
Password:  
[root@rapavlichenko ~]# chmod +t /tmp  
[root@rapavlichenko ~]# exit  
logout  
[guest2@rapavlichenko rapavlichenko]$
```