

Лабораторная работа №5

Основы информационной безопасности

Кондрашова А. А.

6 октября 2022

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19

- 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

- Вошли в систему от имени пользователя guest2.
- Создали программу simpleid.c.
- Скомпилировали программу и убедитесь, что файл программы создан с помощью команды `gcc simpleid.c -o simpleid`.
- Выполните программу simpleid.
- Выполните системную программу `id` и сравнили полученный нами результат с данными предыдущего пункта. Данные идентичны.

```
Last login: Sat Sep 17 20:58:58 MSK 2022 on pts/1
[guest2@maakondrashova ~]$ simpleid.c
bash: simpleid.c: command not found...
[guest2@maakondrashova ~]$ touch simpleid.c
[guest2@maakondrashova ~]$ nano simpleid.c
[guest2@maakondrashova ~]$ gcc simpleid.c -o simpleid
[guest2@maakondrashova ~]$ ./simpleid
uid=1002, gid=1002/n[guest2@maakondrashova ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest
023
```

Figure 1: Выполнение программы simpleid

- Усложнили программу, добавив вывод действительных идентификаторов. Получившуюся программу назвали simpleid2.c.
- Скомпилируйте и запустили simpleid2.c с помощью команды `gcc simpleid2.c -o simpleid2`.

```
[guest2@aakondrashova ~]$ nano simpleid.c
[guest2@aakondrashova ~]$ nano simpleid2.c
[guest2@aakondrashova ~]$ gcc simpleid2.c -o simpleid2
[guest2@aakondrashova ~]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest2@aakondrashova ~]$
```

Figure 2: Выполнение программы simpleid2

Выполнение лабораторной работы

- От имени суперпользователя выполнили команды (для этого использовали повышение своих прав с помощью sudo): `chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2`
- Выполнили проверку правильности установки новых атрибутов и смены владельца файла `simpleid2`.
- Запустите `simpleid2` и `id`.

```
[aakondrashova@aakondrashova ~]$ chown root:guest2 /home/guest2/simpleid2
chown: cannot access '/home/guest2/simpleid2': Permission denied
[aakondrashova@aakondrashova ~]$ sudo chown root:guest2 /home/guest2/simpleid2
[sudo] password for aakondrashova:
[aakondrashova@aakondrashova ~]$ sudo u+s /home/guest2/simpleid2
sudo: u+s: command not found
[aakondrashova@aakondrashova ~]$ sudo chmod u+s /home/guest2/simpleid2
[aakondrashova@aakondrashova ~]$ su - guest2
Password:
Last login: Sat Oct  1 20:58:54 MSK 2022 on pts/1
[guest2@aakondrashova ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest2 80584 Oct  1 21:55 simpleid2
[guest2@aakondrashova ~]$ ./simpleid2
e uid=0, e gid=1002
real_uid=1002, real_gid=1002
[guest2@aakondrashova ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0
023
```

Figure 3: Выполнение программы `simpleid2`

- Создали программу readfile.c:
- Откомпилировали её.

```
[guest2@aakondrashova ~]$ touch readfile.c  
[guest2@aakondrashova ~]$ nano readfile.c  
[guest2@aakondrashova ~]$ gcc readfile.c -o readfile
```

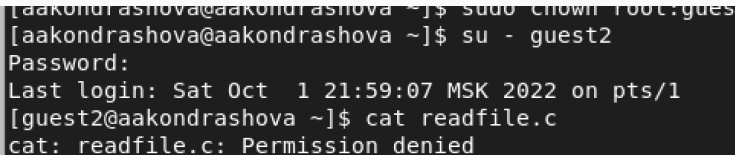
Figure 4: Создание программы readfile.c

- Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest2 не мог.

```
[aakondrashova@aakondrashova ~]$ sudo chmod 700 /home/guest2/readfile.c
[sudo] password for aakondrashova:
Sorry, try again.
[sudo] password for aakondrashova:
[aakondrashova@aakondrashova ~]$ sudo chown root:guest2 /home/guest2/readfile.c
```

Figure 5: Смена прав

- Проверили, что пользователь guest2 не может прочитать файл readfile.c.

A terminal window showing a sequence of commands and their outputs. The user starts as 'aakondrashova', uses 'sudo' to become 'root', then switches to 'guest2' using 'su'. After entering a password, the user runs 'cat readfile.c', which results in a 'Permission denied' error.

```
[aakondrashova@aakondrashova ~]$ sudo -l whoami root:guest2
[aakondrashova@aakondrashova ~]$ su - guest2
Password:
Last login: Sat Oct  1 21:59:07 MSK 2022 on pts/1
[guest2@aakondrashova ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Figure 6: Проверка невозможности чтения

- Сменили у программы readfile владельца и установите SetU'D-бит.

```
Last login: Sat Oct  1 22:21:46 MSK 2022 on pts/1
[aakondrashova@aakondrashova ~]$ sudo chown root:guest2 /home/guest2/readfile.c
[aakondrashova@aakondrashova ~]$ sudo chown u+s /home/guest2/readfile
chown: invalid user: 'u+s'
[aakondrashova@aakondrashova ~]$ sudo chown root:guest2 /home/guest2/readfile
[aakondrashova@aakondrashova ~]$ sudo chown u+s /home/guest2/readfile
chown: invalid user: 'u+s'
[aakondrashova@aakondrashova ~]$ sudo chmod u+s /home/guest2/readfile
```

Figure 7: Смена владельца и установка SetU'D-бит

Выполнение лабораторной работы

- Проверили, что программа readfile может прочитать файл readfile.c

```
Last login: Sat Oct 1 22:24:02 MSK 2022 on pts/1
[guest2@aaakondrashova ~]$ ./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]);
    }
}
```

Figure 8: Проверка возможности чтения файла readfile.c

- Проверьте, что программа readfile может прочитать файл /etc/shadow

[illegible]

Figure 9: Проверка возможности чтения файла /etc/shadow

- Выяснили, установлен ли атрибут Sticky на директории /tmp, для чего выполнили 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».

```
[guest2@maakondrashova ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  1 22:28 tmp
[guest2@maakondrashova ~]$ echo "test" > /tmp/file01.txt
[guest2@maakondrashova ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest2 guest2 5 Oct  1 22:29 /tmp/file01.txt
[guest2@maakondrashova ~]$ chmod o+rw /tmp/file01.txt
[guest2@maakondrashova ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest2 guest2 5 Oct  1 22:29 /tmp/file01.txt
```

Figure 10: Атрибуты на директории /tmp и файла file01.txt

Исследование Sticky-бита

- От пользователя guest3 (не являющегося владельцем) попробовали прочитать файл /tmp/file01.txt. Нам это удалось.
- От пользователя guest3 попробовали дозаписать в файл /tmp/file01.txt слово test2. Слово перезаписалось, а не дозаписалось.
- От пользователя guest3 попробовали перезаписать в файл /tmp/file01.txt слово test3. Слово перезаписалось.
- От пользователя guest3 попробовали удалить файл /tmp/file01.txt командой
- Повысили свои права до суперпользователя и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp.

```
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test
[guest3@aakondrashova ~]$ echo "test2" > /tmp/file01.txt
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test2
[guest3@aakondrashova ~]$ echo "test3" > /tmp/file01.txt
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test3
[guest3@aakondrashova ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest3@aakondrashova ~]$ su -
Password:
[root@aakondrashova ~]# chmod -t /tmp
[root@aakondrashova ~]# exit
logout
```

- От пользователя guest3 проверили, что атрибута t у директории /tmp нет.
- Повторили предыдущие шаги, удалось удалить файл.
- Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp:

```
[guest3@aakondrashova ~]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  1 22:35 tmp
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test3
[guest3@aakondrashova ~]$ echo "test2" > /tmp/file01.txt
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test2
[guest3@aakondrashova ~]$ echo "test3" > /tmp/file01.txt
[guest3@aakondrashova ~]$ cat /tmp/file01.txt
test3
[guest3@aakondrashova ~]$ rm /tmp/file01.txt
[guest3@aakondrashova ~]$ su -
Password:
Last login: Sat Oct  1 22:34:34 MSK 2022 on pts/1
[root@aakondrashova ~]# chmod +t /tmp
[root@aakondrashova ~]# exit
logout
[guest3@aakondrashova ~]$
```

Figure 12: Атрибут t

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.