

Лабораторная работа №5

Основы информационной безопасности


Мишина А. А.

11 апреля 2024

- Мишина Анастасия Алексеевна
- НПИбд-02-22

Выполнение 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.



```
guest@aamishina:~  
[aamishina@aamishina ~]$ su guest  
Password:  
[guest@aamishina aamishina]$ cd  
[guest@aamishina ~]$ touch simpleid.c  
[guest@aamishina ~]$ vi simpleid.c  
[guest@aamishina ~]$
```

Рис. 1: Создание файла simpleid.c



```
guest@aamishina:~ — /usr/bin/vim simpleid.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;
}
```

Рис. 2: Программа в файле simpleid.c

```
[guest@aamishina ~]$ gcc simpleid.c -o simpleid
[guest@aamishina ~]$ ls -l
total 28
drwxrwxrwx. 2 guest guest   72 Mar 27 14:11 .
-rwxr-xr-x. 1 guest guest 80672 Apr 11 12:45 simpleid
-rw-r--r--. 1 guest guest  176 Apr 11 12:45 simpleid.c
[guest@aamishina ~]$ ./simpleid
uid=1001, gid=1001
[guest@aamishina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
[guest@aamishina ~]$
```

Рис. 3: Выполнение программы simpleid и команды id



```
guest@aamishina:~ — /usr/bin/vim simpleid.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;
}
```

Рис. 4: Добавление вывода действительных идентификаторов


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

Рис. 5: Компиляция и запуск simpleid2

Смена атрибута и владельца

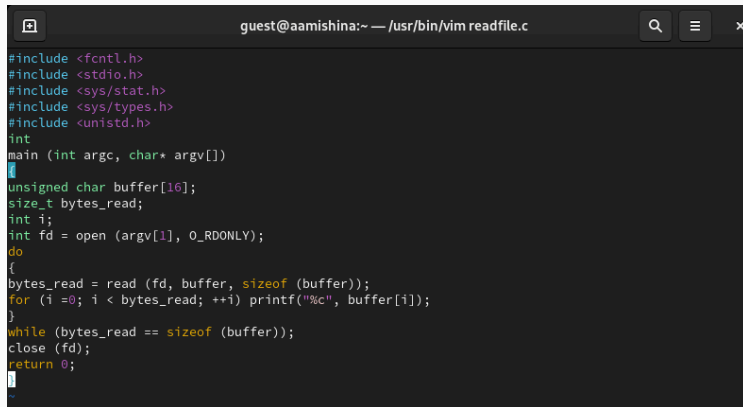
```
[guest@aamishina ~]$ su -  
Password:  
Last login: Wed Mar 27 14:07:45 MSK 2024 on pts/1  
Last failed login: Thu Apr 11 12:49:54 MSK 2024 on pts/0  
There was 1 failed login attempt since the last successful login.  
[root@aamishina ~]#  
[root@aamishina ~]#  
[root@aamishina ~]# chown root:guest /home/guest/simpleid2  
[root@aamishina ~]# chmod u+s /home/guest/simpleid2  
[root@aamishina ~]# exit  
logout  
[guest@aamishina ~]$ ls -l simpleid2  
-rwsr-xr-x. 1 root guest 80768 Apr 11 12:49 simpleid2  
[guest@aamishina ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@aamishina ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:  
s0-s0:c0.c1023  
[guest@aamishina ~]$
```

Рис. 6: Запуск simpleid2 с SETUID. Сравнение результатов

Смена атрибута и владельца

```
[guest@aamishina ~]$ su -
Password:
Last login: Thu Apr 11 12:50:01 MSK 2024 on pts/0
[root@aamishina ~]# chmod u-s /home/guest/simpleid2
[root@aamishina ~]# chmod g+s /home/guest/simpleid2
[root@aamishina ~]# exit
logout
[guest@aamishina ~]$ ls -l simpleid2
-rwxr-sr-x. 1 root guest 80768 Apr 11 12:49 simpleid2
[guest@aamishina ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@aamishina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
[guest@aamishina ~]$
```

Рис. 7: Запуск simpleid2 с SETGID. Сравнение результатов



```
guest@aamishina:~ — /usr/bin/vim 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]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

Рис. 8: Программа readfile

```
[guest@aamishina ~]$ gcc readfile.c -o readfile
[guest@aamishina ~]$ sudo chown root:guest /home/guest/readfile.c

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for guest:
guest is not in the sudoers file. This incident will be reported.
[guest@aamishina ~]$ su -
Password:
Last login: Thu Apr 11 12:53:04 MSK 2024 on pts/0
[root@aamishina ~]# sudo chown root:guest /home/guest/readfile.c
[root@aamishina ~]# chmod 700 /home/guest/readfile.c
[root@aamishina ~]# exit
logout
[guest@aamishina ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@aamishina ~]$
```

Рис. 9: Изменение прав доступа, проверка от имени пользователя guest

Смена владельца и атрибута

```
[guest@aaamishina ~]$ su -
Password:
Last login: Thu Apr 11 12:57:53 MSK 2024 on pts/0
[root@aaamishina ~]# chown root:guest /home/guest/readfile
[root@aaamishina ~]# chmod u+s /home/guest/readfile
[root@aaamishina ~]# exit
logout
[guest@aaamishina ~]$ ./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[10];
    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;
}
[guest@aaamishina ~]$ ./readfile /etc/shadow
root:$6$Lum1r0dHjK02lsdIrcrf7zyY6vBkHgc8L0d2X5kzVRk4ca3MwVFEZFZmWkCroiEUtrv4GQJZct/GTqAPtE
ndn01ZFCxwz;0:99999:7:::
bini:*19469:0:99999:7:::
daemon:*19469:0:99999:7:::
adm:*19469:0:99999:7:::
lp:*19469:0:99999:7:::
sync:*19469:0:99999:7:::
shutdown:*19469:0:99999:7:::
halt:*19469:0:99999:7:::
nail:*19469:0:99999:7:::
operator:*19469:0:99999:7:::
games:*19469:0:99999:7:::
ftp:*19469:0:99999:7:::
nobody:*19469:0:99999:7:::
systemd-coredump:!:19769:!!!!:
dbus:!:19769:!!!!:
polkitd:!:19769:!!!!:
wpaht:!:19769:!!!!:
```

Рис. 10: Установка SETUID для readfile, проверка

```
[guest@aamishina ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Apr 11 13:03 tmp
[guest@aamishina ~]$ echo "test" > /tmp/file01.txt
[guest@aamishina ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Apr 11 13:06 /tmp/file01.txt
[guest@aamishina ~]$ chmod o+rw /tmp/file01.txt
[guest@aamishina ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Apr 11 13:06 /tmp/file01.txt
[guest@aamishina ~]$ su guest2
Password:
[guest2@aamishina guest]$ cat /tmp/file01.txt
test
[guest2@aamishina guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aamishina guest]$ cat /tmp/file01.txt
test
[guest2@aamishina guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aamishina guest]$ cat /tmp/file01.txt
test
[guest2@aamishina guest]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aamishina guest]$ cat /tmp/file01.txt
test
[guest2@aamishina guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@aamishina guest]$ cd
[guest2@aamishina ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@aamishina ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@aamishina ~]$
```

Рис. 11: Проверка наличия атрибута Sticky на /tmp, работа с файлом file01.txt

```
[guest2@aamishina ~]$ su -  
Password:  
Last login: Thu Apr 11 13:03:10 MSK 2024 on pts/0  
[root@aamishina ~]# chmod -t /tmp  
[root@aamishina ~]# exit  
logout  
[guest2@aamishina ~]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 Apr 11 13:09 tmp  
[guest2@aamishina ~]$ cat /tmp/file01.txt  
test  
[guest2@aamishina ~]$ echo "test2" > /tmp/file01.txt  
bash: /tmp/file01.txt: Permission denied  
[guest2@aamishina ~]$ echo "test3" >> /tmp/file01.txt  
bash: /tmp/file01.txt: Permission denied  
[guest2@aamishina ~]$ rm /tmp/file01.txt  
rm: remove write-protected regular file '/tmp/file01.txt'? y
```

Рис. 12: Снятие атрибута t (Sticky-бит), повторение операций


```
[guest2@aamishina ~]$  
[guest2@aamishina ~]$ ls -l /tmp | grep file01  
[guest2@aamishina ~]$  
[guest2@aamishina ~]$  
[guest2@aamishina ~]$ su -  
Password:  
Last login: Thu Apr 11 13:09:57 MSK 2024 on pts/0  
[root@aamishina ~]# chmod +t /tmp  
[root@aamishina ~]# exit  
logout  
[guest2@aamishina ~]$
```

Рис. 13: Возвращение атрибута

- В ходе выполнения данной лабораторной работы, я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.