

Презентация по лабораторной работе №5

Основы информационной безопасности

Мажитов М. А.

28 сентября 2024

Российский университет дружбы народов, Москва, Россия

- Мажитов Магомед Асхабович
- студент группы НКНбд-01-21
- Российский университет дружбы народов



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.

Проверил установлен ли компилятор gcc и g++.

```
[mamazhitov@localhost ~]$ gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/8/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enable-shared --enable-threads=posix --enable-checking=release --enable-multilib --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --with-linker-hash-style=gnu --enable-plugin --enable-initfini-array --with-isl --disable-libmpx --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Модель многопоточности: posix
gcc версия 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)
[mamazhitov@localhost ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[mamazhitov@localhost ~]$ S
```

Рис. 1: Компилятор

Вошел в систему от имени пользователя guest и создал программу simpleid.c.

```
[guest@localhost home]$ cd guest  
[guest@localhost ~]$ touch simpleid.c  
[guest@localhost ~]$ nano simpleid.c
```

Рис. 2: Создание simpleid.c



```
GNU nano 2.9.8 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. 3: Код программы simpleid.c

Скомпилировал программу и убедился, что файл программы создан. Далее запустил исполняемый файл, а также ввел системную программу *id* для дальнейшего сравнения выводов.

```
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ls
dir1  simpleid  simpleid.c
[guest@localhost ~]$ nano simpleid.c
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$
```

Рис. 4: Компиляция simpleid.c

Результаты идентичны.

Создал программу *simpleid2.c*.

```
[guest@localhost ~]$ touch simpleid2.c  
[guest@localhost ~]$ nano simpleid2.c  
[guest@localhost ~]$
```

Рис. 5: Создание simpleid2.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;  
}
```

Скомпилировал программу и сравнил выводы прошлой и новой программ.

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

Рис. 7: Сравнение

Далее я поменял владельца файла *simpleid2* и изменил права доступа к нему.

```
[root@localhost home]# chown root:guest /home/guest/simpleid2
[root@localhost home]# chmod u+s /home/guest/simpleid2
[root@localhost home]# cd guest
[root@localhost guest]# ls -l
итого 48
drwxr-xr-x. 2 guest guest    19 сен 28 21:33 dir1
-rwxrwxr-x. 1 guest guest 18208 окт  5 21:46 simpleid
-rwsrwxr-x. 1 root  guest 18312 окт  5 21:53 simpleid2
-rw-rw-r--. 1 guest guest   302 окт  5 21:53 simpleid2.c
-rw-rw-r--. 1 guest guest   175 окт  5 21:46 simpleid.c
[root@localhost guest]#
```

Рис. 8: Манипуляции simpleid2

Запустил *simpleid2* и *id*.

```
[guest@localhost ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$
```

Рис. 9: Сравнение

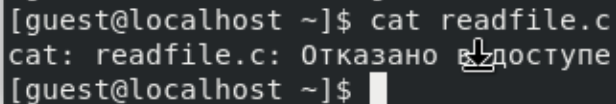
Как мы видим после изменения владельца *simpleid2*, вывод программы изменился.

Создал программу *readfile.c*. Скомпилировал файл и далее также изменил владельца *readfile* и права доступа к нему, так, чтобы только суперпользователь(root) мог прочитать его, а guest не мог.

```
[root@localhost guest]# chown root:guest /home/guest/readfile.c
[root@localhost guest]# chmod 700 readfile.c
[root@localhost guest]# chmod -u readfile.c
[root@localhost guest]# chmod u+s readfile.c
[root@localhost guest]# ls -l
итого 72
drwxr-xr-x. 2 guest guest    19 сен 28 21:33 dir1
-rwxrwxr-x. 1 guest guest 18256 окт  5 22:02 readfile
---S----- 1 root  guest   402 окт  5 22:01 readfile.c
-rwxrwxr-x. 1 guest guest 18208 окт  5 21:46 simpleid
-rwsrwxr-x. 1 root  guest 18312 окт  5 21:53 simpleid2
-rw-rw-r-- 1 guest guest   302 окт  5 21:53 simpleid2.c
-rw-rw-r-- 1 guest guest   175 окт  5 21:46 simpleid.c
[root@localhost guest]#
```

Рис. 10: Изменение владельца *readfile*

Попробовал прочитать файл от имени *guest*.

A terminal window with a dark background and light gray text. The prompt is [guest@localhost ~]\$. The user enters 'cat readfile.c'. The output is 'cat: readfile.c: Отказано в доступе'. The prompt returns as [guest@localhost ~]\$.

```
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@localhost ~]$
```

Рис. 11: Попытка прочитать readfile

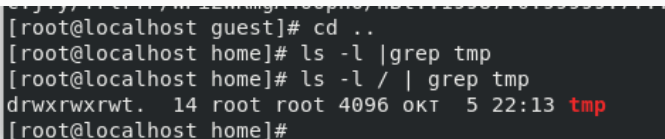
Попытка не увенчалась успехом.

Проверил, может ли программа `readfile` прочитать файл `readfile.c` и `/etc/shadow`.

```
[root@localhost guest]# ./readfile readfile.c
[root@localhost guest]# eof (buffer));("%c", buffer[i]);
[root@localhost guest]# ./readfile /etc/shadow
root:$6$UpDUSH.jEJNgJAn8$IHiyHMum3xzH4a7yb67E0uYWBzBt9WB.9ZyQKYyjA1V30.p9ojwqAai
20ck80vhxGmGN7vXeMBuCPPncY6ojv.:0:99999:7:::
bin:*:19767:0:99999:7:::
daemon:*:19767:0:99999:7:::
adm:*:19767:0:99999:7:::
```

Рис. 12: Попытка запустить `readfile`

Проверил, установлен ли атрибут *Sticky* на директории /tmp.



```
[root@localhost guest]# cd ..  
[root@localhost home]# ls -l |grep tmp  
[root@localhost home]# ls -l / | grep tmp  
drwxrwxrwt. 14 root root 4096 окт 5 22:13 tmp  
[root@localhost home]#
```

Рис. 13: Проверка наличия Sticky атрибута

От имени пользователя *guest* создал файл *file01.txt* в директории */tmp* со словом *test* и изменил права доступа к нему.

```
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 окт  5 23:00 /tmp/file01.txt
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  5 23:00 /tmp/file01.txt
[guest@localhost ~]$
```

Рис. 14: Создание *file01.txt*

От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл, переписать содержимое файла, а также дописать в файл новые данные.

```
[guest2@localhost mamazhitov]$ cd ..  
[guest2@localhost home]$ cat /tmp/file01.txt  
test  
[guest2@localhost home]$ echo "test2" > /tmp/file01.txt  
[guest2@localhost home]$ cat /tmp/file01.txt  
test2  
[guest2@localhost home]$ S
```

Рис. 15: Манипуляции с file01.txt

Попробовал удалить файл.

```
test3  
[guest2@localhost home]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@localhost home]$
```

Рис. 16: Попытка удалить file01.txt

Повысив права до суперпользователя, снял атрибут *t*.

```
[root@localhost home]# chmod -t /tmp
[root@localhost home]# ls -l /tmp
итого 4
-rw-rw-rw-. 1 guest      guest      12 окт  5 22:20 file01.txt
drwx----- 3 root       root       17 окт  5 21:34 systemd-private-68
drwx----- 3 root       root       17 окт  5 21:34 systemd-private-68
drwx----- 3 root       root       17 окт  5 21:36 systemd-private-68
drwx----- 3 root       root       17 окт  5 21:34 systemd-private-68
cV
drwx----- 3 root       root       17 окт  5 21:34 systemd-private-68
Z6
drwx----- 2 mamazhitov mamazhitov  6 окт  5 21:37 Temp-561bb308-5a4a
[root@localhost home]# ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 окт  5 22:21 tmp
[root@localhost home]#
```

Рис. 17: Снятие атрибута *t*

Повторил действия из пунктов 13-14.

```
[guest2@localhost home]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 окт  5 22:21 tmp
[guest2@localhost home]$ cat /tmp/file01.txt
test2
test3
[guest2@localhost home]$ echo "test2" > /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01.txt
test2
[guest2@localhost home]$ echo "test3" >> /tmp/file01.txt
[guest2@localhost home]$ cat /tmp/file01.txt
test2
test3
[guest2@localhost home]$ rm /tmp/file01.txt
[guest2@localhost home]$ ls /tmp
systemd-private-684e72e4d3364f87b633fd6f3cbd2be3-chrond.service-2xjhxM
systemd-private-684e72e4d3364f87b633fd6f3cbd2be3-colord.service-RTxSqC
systemd-private-684e72e4d3364f87b633fd6f3cbd2be3-fwupd.service-vwFWTH
systemd-private-684e72e4d3364f87b633fd6f3cbd2be3-ModemManager.service-BZGxcV
systemd-private-684e72e4d3364f87b633fd6f3cbd2be3-rtkit-daemon.service-h3VPZ6
Temp-561bb308-5a4a-494a-aaaf-5104105da6e7
[guest2@localhost home]$
```

Рис. 18: Манипуляции с file01.txt

В этот раз получилось удалить *file01.txt*.

Попробовал удалить файл.

```
test3  
[guest2@localhost home]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@localhost home]$
```

Рис. 19: Попытка удалить file01.txt

Изучил механизм изменения идентификаторов, применил SetUID- и Sticky-биты. Получил практические навыки 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. Библиография