РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

Дисциплина: Информационная безопасность

Тема: Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Студент: Ломакина София Васильевна

Группа: НФИбд-02-19

МОСКВА

2022 г.

Цель работы **2**

Выполнение лабораторной работы **2**

Подготовка лабораторного стенда 2

Создание программы 3

Исследование Sticky-бита 8

Вывод **10**

Цель 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.

Выполнение лабораторной работы

Подготовка лабораторного стенда

Убедилась, что в системе установлен компилятор gcc, введя команду gcc -v. Также проверила отключение систему запретов до очередной перезагрузки системы командой getenforce, которая вывела Permissive.

```
[sofa@sofa ~]$ gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/4.8.5/lto-wrapper
Target: x86_64-redhat-linux
Configured with: ../configure --prefix=/usr --mandir=/usr/share/man --infodir=/usr/shar
e/info --with-bugurl=http://bugzilla.redhat.com/bugzilla --enable-bootstrap --enable-sh
ared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-__cxa
_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build
-id --with-linker-hash-style=gnu --enable-languages=c,c++,objc,obj-c++,java,fortran,ada
,go,lto --enable-plugin --enable-initfini-array --disable-libgcj --with-isl=/builddir/b
uild/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/isl-install --with-cloog=/builddi
r/build/BUILD/gcc-4.8.5-20150702/obj-x86_64-redhat-linux/cloog-install --enable-gnu-ind
irect-function --with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Thread model: posix
gcc version 4.8.5 20150623 (Red Hat 4.8.5-44) (GCC)
```

```
[sofa@sofa ~]$ sudo setenforce 0
[sudo] password for sofa:
[sofa@sofa ~]$ getenforce
Permissive
```

Создание программы

Вошла в систему от имени пользователя guest и создала программу simpleid.c со следующим кодом:

```
[sofa@sofa ~]$ su guest
Password:
[guest@sofa sofa]$ ls
ls: cannot open directory .: Permission denied
[guest@sofa sofa]$ cd ..
[guest@sofa home]$ ls
guest  guest2  sofa
[guest@sofa home]$ cd guest
[guest@sofa ~]$ ls
dir1
[guest@sofa ~]$ touch simpleid.c
[guest@sofa ~]$ ls
dir1  simpleid.c
[guest@sofa ~]$ vim simpleid.c
[guest@sofa ~]$ cat simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main() {
        uid_t uid = getuid();
        gid_t gid = getgid();
        printf("uid=%d, gid=%d\n", uid, gid);
        return 0;
}
```

Скомпилировала программу с помощью команды gcc simpleid.c -o simpleid и убедилась, что файл программы создан. Выполнила программу simpleid, а также системную программу id. Результат выполнения двух последних программ одинаков.

```
[guest@sofa ~]$ gcc simpleid.c -o simpleid
[guest@sofa ~]$ ls
dir1  simpleid  simpleid.c
[guest@sofa ~]$ ./simpleid
uid=1001, gid=1001
[guest@sofa ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023
```

Усложнила программу, добавив вывод действительных идентификаторов и назвала получившуюся программу simpleid2.c.

```
[guest@sofa ~]$ vim simpleid.c
[guest@sofa ~]$ mv simpleid.c simpleid2.c
[guest@sofa ~]$ cat 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;
}
```

Скомпилировала и запустила simpleid2.c.

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

От имени суперпользователя выполните команды chown root:guest /home/guest/simpleid2 и chmod u+s /home/guest/simpleid2, повысив права пользователя с помощью команды su и изменив владельца и атрибуты simpleid2.
Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой ls -l simpleid2, а также запустила simpleid2 и id. Результат выполнения программ отличается, поскольку программа simpleid2 выводит uid и gid владельца, а команда id - uid и gid текущего пользователя.

```
[guest@sofa ~]$ su sofa
Password:
[sofa@sofa guest]$ chown root:guest /home/guest/simpleid2
chown: cannot access ‘/home/guest/simpleid2’: Permission denied
[sofa@sofa guest]$ sudo chown root:guest /home/guest/simpleid2
[sudo] password for sofa:
[sofa@sofa guest]$ sudo chmod u+s /home/guest/simpleid2
[sofa@sofa guest]$ ls -l simpleid2
ls: cannot access simpleid2: Permission denied
[sofa@sofa guest]$ sudo ls -l simpleid2
-rwsrwxr-x. 1 root guest 8616 Oct  8 20:20 simpleid2
[sofa@sofa guest]$ su guest
Password:
[guest@sofa ~]$ ls
dir1  simpleid  simpleid2  simpleid2.c
[guest@sofa ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@sofa ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023
```

Проделала то же самое относительно SetGID-бита.

```
[root@sofa guest]# chmod g+s /home/guest/simpleid2
[root@sofa guest]# exit
exit
[guest@sofa ~]$ ls -l simpleid2
-rwsrwsr-x. 1 root guest 8616 Oct  8 20:20 simpleid2
[guest@sofa ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@sofa ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023
[guest@sofa ~]$
```

Создала программу readfile.c.

```
[guest@sofa ~]$ cat readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/types.h>
#include <sys/stat.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;
}
```

Откомпилируйте программу с помощью команды gcc readfile.c -o readfile. После от имени администратора сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог. Проверила, что пользователь guest не может прочитать файл readfile.c.

```
[guest@sofa ~]$ gcc readfile.c -o readfile
[guest@sofa ~]$ su
Password:
[root@sofa guest]# chown root:guest /home/guest/readfile.c
[root@sofa guest]# chmod ug-r /home/guest/readfile.c
[root@sofa guest]# exit
exit
[guest@sofa ~]$ ls -l readfile.c
--w--w-r--. 1 root guest 423 Oct  8 20:34 readfile.c
[guest@sofa ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Сменила у программы readfile владельца и установила SetUID-бит. Выяснила, что программа readfile не может прочитать файл readfile.c.

Также выяснила, что программа readfile не может прочитать файл /etc/shadow.

Исследование Sticky-бита

Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ls -l / | grep tmp. Атрибут установлен. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test с помощью команды echo “test” > /tmp/file01.txt. После просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» с помощью команд ls -l /tmp/file01.txt, chmod o+rw /tmp/file01.txt и ls -l /tmp/file01.txt.

```
[guest@sofa ~]$ ls -l / | grep tmp
drwxrwxrwt.  21 root root 4096 Oct  8 20:41 tmp
[guest@sofa ~]$ echo "test" > /tmp/file01.txt
[guest@sofa ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 20:44 /tmp/file01.txt
[guest@sofa ~]$ chmod o+rw /tmp/file01.txt
[guest@sofa ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 20:44 /tmp/file01.txt
```

От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt с помощью команды cat /tmp/file01.txt. После попробовала дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” > /tmp/file01.txt. Проверила содержимое файла командой cat /tmp/file01.txt. Далее попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt. Снова проверила содержимое файла командой cat /tmp/file01.txt. Попробовала удалить файл /tmp/file01.txt командой rm /tmp/file01.txt. Получилось выполнить все команды на запись и чтение, но не команду удаления файла.

```
[guest@sofa ~]$ su guest2
Password:
[guest2@sofa guest]$ cat /tmp/file01.txt
test
[guest2@sofa guest]$ echo "test2" > /tmp/file01.txt
[guest2@sofa guest]$ cat /tmp/file01.txt
test2
[guest2@sofa guest]$ echo "test2" >> /tmp/file01.txt
[guest2@sofa guest]$ cat /tmp/file01.txt
test2
test2
[guest2@sofa guest]$ echo "test3" > /tmp/file01.txt
[guest2@sofa guest]$ cat /tmp/file01.txt
test3
[guest2@sofa guest]$ rm /tmp/file01/txt
rm: cannot remove ‘/tmp/file01/txt’: No such file or directory
[guest2@sofa guest]$ rm /tmp/file01.txt
rm: cannot remove ‘/tmp/file01.txt’: Operation not permitted
```

Повысила свои права до суперпользователя командой su - и выполнила команду chmod -t /tmp, снимающую атрибут t (Sticky-бит) с директории /tmp. Покинула режим суперпользователя командой exit.

```
[guest2@sofa guest]$ su
Password:
[root@sofa guest]# chmod -t /tmp
[root@sofa guest]# exit
exit
[guest2@sofa guest]$
```

От пользователя guest2 проверила командой ls -l / | grep tmp, что атрибута t у директории /tmp нет. Повторила предыдущие шаги, причем в этот раз удалось удалить файл от имени пользователя, не являющегося владельцем файла file01.txt.

```
[guest2@sofa guest]$ ls -l / | grep tmp
drwxrwxrwx.  21 root root 4096 Oct  8 20:50 tmp
[guest2@sofa guest]$ cat /tmp/file01.txt
test3
[guest2@sofa guest]$ echo "test" >> /tmp/file01.txt
[guest2@sofa guest]$ cat /tmp/file01.txt
test3
test
[guest2@sofa guest]$ echo "test2" > /tmp/file01.txt
[guest2@sofa guest]$ cat /tmp/file01.txt
test2
[guest2@sofa guest]$ rm /tmp/file01.txt
```

Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp.

```
[guest2@sofa guest]$ su
Password:
[root@sofa guest]# chmod +t /tmp
[root@sofa guest]# exit
exit
[guest2@sofa guest]$ ls -l / | grep tmp
drwxrwxrwt.  21 root root 4096 Oct  8 20:54 tmp
```

Вывод

В ходе выполнения лабораторной работы были изучены механизмы изменения

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