

Лабораторная работа №5

Информационная безопасность

Маметкадыров Ынтымак | НПМбд-02-20

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
3.1	Создание программы	6
3.2	3.2 Исследование Sticky-бита	11
4	Выводы	14
	Список литературы	15

Список иллюстраций

3.1	Предварительная подготовка	6
3.2	Команда “whereis”	6
3.3	Вход в систему и создание программы	7
3.4	Код программы simpleid.c	7
3.5	Компиляция и выполнение программы simpleid	8
3.6	Усложнение программы	8
3.7	Создание файла simpleid2.c	8
3.8	Компиляция и выполнение программы simpleid2	9
3.9	Установка новых атрибутов (SetUID) и смена владельца файл . . .	9
3.10	Запуск simpleid2 после установки SetUID	9
3.11	Запуск simpleid2 после установки SetGID	10
3.12	Смена владельца и прав доступа у файла readfile.c	10
3.13	Запуск программы readfile	11
3.14	Создание файла file01.txt	11
3.15	Попытка выполнить действия над файлом file01.txt от имени пользователя guest2	12
3.16	Удаление атрибута t (Sticky-бита) и повторение действий	13
3.17	Возвращение атрибута t (Sticky-бита)	13

1 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.

2 Теоретическое введение

SetUID, SetGID и Sticky — это специальные типы разрешений, которые позволяют задавать расширенные права доступа на файлы и каталоги.

- SetUID — это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволят поднять привилегии пользователя в случае, если это необходимо. Наличие SetUID бита выражается в том, что на месте классического бита x выставлен специальный бит s: `-rwsr-xr-x`
- SetGID — очень похож на SetUID с отличием, что файл будет запускаться от имени группы, который владеет файлом: `-rwxr-sr-x`
- Sticky — в случае, если этот бит установлен для папки, то файлы в этой папке могут быть удалены только их владельцем. Наличие этого бита показывается через букву t в конце всех прав: `drwxrwxrwx`

Более подробно см. в [1].

3 Выполнение лабораторной работы

3.1 Создание программы

Для начала убедились, что компилятор gcc установлен, используя команду “gcc -v”. Затем отключили систему запретов до очередной перезагрузки системы командой “sudo setenforce 0”, после чего команда “getenforce” вывели “Permissive” (рис. 3.1)

```
[itmametkadirov@itmametkadirov ~]$ gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --enable-host-pie --enable-host-bind-now --
--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-check
ing-release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-u
nique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initf
ini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nv
ptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --w
ith-arch_64=x86-64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootst
rap-lto --enable-link-serialization=1
Модель многопоточности: posix
Supported LTO compression algorithms: zlib zstd
gcc версия 11.3.1 20221121 (Red Hat 11.3.1-4) (GCC)
[itmametkadirov@itmametkadirov ~]$ sudo setenforce 0
[sudo] пароль для itmametkadirov:
[itmametkadirov@itmametkadirov ~]$ getenforce
Permissive
```

Рис. 3.1: Предварительная подготовка

Проверили успешное выполнение команд. (рис. 3.2)

```
[itmametkadirov@itmametkadirov ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.i
nfo.gz
[itmametkadirov@itmametkadirov ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
```

Рис. 3.2: Команда “whereis”

Вошли в систему от имени пользователя guest командой “su - guest”. Создали

программу simpleid.c командой “touch simpleid.c” и открыли её в редакторе командой “gedit /home/guest/simpleid.c” (рис. 3.3)

```
itmametkadirov@itmametkadirov ~]$ su - guest
Пароль:
[guest@itmametkadirov ~]$ touch simpleid.c
[guest@itmametkadirov ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
simpleid.c  Документы  Изображения  Общедоступные  Шаблоны
[guest@itmametkadirov ~]$ gedit /home/guest/simpleid.c

(gedit:3174): dbind-WARNING **: 13:22:43.285: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

(gedit:3174): dconf-WARNING **: 13:22:43.530: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:3174): dconf-WARNING **: 13:22:43.545: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:3174): dconf-WARNING **: 13:22:44.928: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:3174): dconf-WARNING **: 13:22:44.929: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:3174): dconf-WARNING **: 13:22:44.929: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
```

Рис. 3.3: Вход в систему и создание программы

Код программы выглядит следующим образом (рис. 3.4).

```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t uid = geteuid ();
9     gid_t gid = getegid ();
10    printf ("uid=%d, gid=%d\n", uid, gid);
11    return 0;
12 }
```

Рис. 3.4: Код программы simpleid.c

Скомпилировали программу и убедились, что файл программы был создан командой “gcc simpleid.c -o simpleid”. Выполнили программу simpleid командой “./simpleid”, а затем выполнили системную программу id командой “id”. Результаты, полученные в результате выполнения обеих команд, совпадают (uid=1001 и gid=1001) (рис. 3.5).

```
[guest@itmametkadihrov ~]$ gcc simpleid.c -o simpleid
[guest@itmametkadihrov ~]$ ./simpleid
uid=1001, gid=1001
[guest@itmametkadihrov ~]$ id
uid=1001(guest) gid=1001(guest) rpyны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t
:s0-s0:c0.c1023
[guest@itmametkadihrov ~]$
```

Рис. 3.5: Компиляция и выполнение программы simpleid

Усложнили программу, добавив вывод действительных идентификаторов (рис. 3.6).

```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t real_uid = geteuid ();
9     uid_t e_uid = geteuid ();
10
11     gid_t real_gid = getgid ();
12     gid_t e_gid = getegid ();
13
14     printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
15     printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
16
17     return 0;
18 }
```

Рис. 3.6: Усложнение программы

Получившуюся программу назвали simpleid2.c (рис. 3.7).

```
[guest@itmametkadihrov ~]$ touch simpleid2.c
[guest@itmametkadihrov ~]$ gedit /home/guest/simpleid.c

(gedit:5116): dbind-WARNING **: 18:18:27.844: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

(gedit:5116): dconf-WARNING **: 18:18:27.243: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:5116): dconf-WARNING **: 18:18:27.278: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:5116): dconf-WARNING **: 18:18:27.992: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:5116): dconf-WARNING **: 18:18:27.992: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:5116): dconf-WARNING **: 18:18:27.993: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

(gedit:5116): dconf-WARNING **: 18:19:02.393: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
[guest@itmametkadihrov ~]$ gedit /home/guest/simpleid.c

(gedit:5160): dbind-WARNING **: 18:19:08.598: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
```

Рис. 3.7: Создание файла simpleid2.c

Скомпилировали и запустили simpleid2.c командами “gcc simpleid2.c -o simpleid2” и “./simpleid2” (рис. 3.8).

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

Рис. 3.8: Компиляция и выполнение программы simpleid2

От имени суперпользователя выполнили команды “sudo chown root:guest /home/guest/simpleid2” и “sudo chmod u+s /home/guest/simpleid2”, затем выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “sudo ls -l /home/guest/simpleid2” (рис. 3.9). Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит.

```
[itmametkadihrov@itmametkadihrov ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для itmametkadihrov:
[itmametkadihrov@itmametkadihrov ~]$ sudo chmod u+s /home/guest/simpleid2
[itmametkadihrov@itmametkadihrov ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 26016 окт  6 18:27 /home/guest/simpleid2
[itmametkadihrov@itmametkadihrov ~]$
```

Рис. 3.9: Установка новых атрибутов (SetUID) и смена владельца файл

Запустили программы simpleid2 и id. Теперь появились различия в uid (рис. 3.10)

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

Рис. 3.10: Запуск simpleid2 после установки SetUID

Проделали тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом (рис. 3.11).

```
[itmametskadihrov@itmametskadihrov ~]$ sudo chown root:guest /home/guest/simpleid2
[itmametskadihrov@itmametskadihrov ~]$ sudo chmod g+s /home/guest/simpleid2
[itmametskadihrov@itmametskadihrov ~]$

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

Рис. 3.11: Запуск simpleid2 после установки SetGID

Создаем программу readfile.c.

Скомпилировали созданную программу командой “gcc readfile.c -o readfile”. Сменили владельца у файла readfile.c командой “sudo chown root:guest /home/guest/readfile.c” и поменяли права так, чтобы только суперпользователь мог прочитать его, а guest не мог, с помощью команды “sudo chmod 700 /home/guest/readfile.c”. Теперь убедились, что пользователь guest не может прочитать файл readfile.c командой “cat readfile.c”, получив отказ в доступе (рис. 3.12).

```
[guest@itmametskadihrov ~]$ touch readfile.c
[guest@itmametskadihrov ~]$ gedit /home/guest/readfile.c

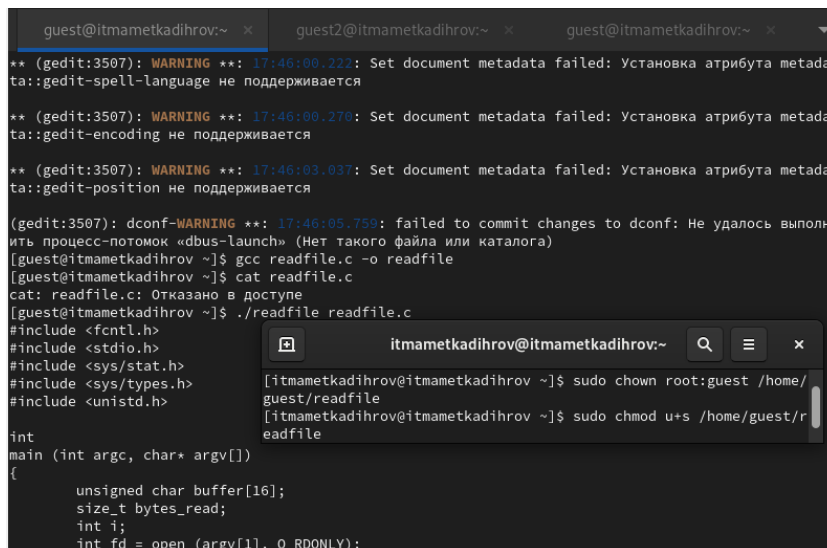
(gedit:3507): dbind-WARNING **: 17:38:38.485: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

(gedit:3507): dconf-WARNING **: 17:38:38.626: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)

itmametskadihrov@itmametskadihrov:~
[itmametskadihrov@itmametskadihrov ~]$ sudo chown root:guest /home/guest/readfile.c
[sudo] пароль для itmametskadihrov:
[itmametskadihrov@itmametskadihrov ~]$ sudo chmod 700 /home/guest/readfile.c
```

Рис. 3.12: Смена владельца и прав доступа у файла readfile.c

Поменяла владельца у программы readfile и установила SetUID. Проверила, может ли программа readfile прочитать файл readfile.c командой “./readfile readfile.c”. Прочитать удалось. Аналогично проверила, можно ли прочитать файл /etc/shadow. Прочитать удалось (рис. 3.13).



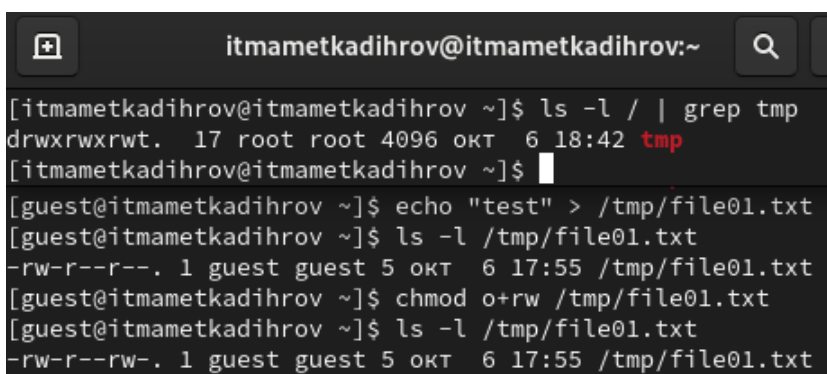
```
guest@itmametskadihrov:~ x guest2@itmametskadihrov:~ x guest@itmametskadihrov:~ x
** (gedit:3507): WARNING **: 17:46:00.222: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:3507): WARNING **: 17:46:00.270: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:3507): WARNING **: 17:46:03.037: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
(gedit:3507): dconf-WARNING **: 17:46:05.759: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
[guest@itmametskadihrov ~]$ gcc readfile.c -o readfile
[guest@itmametskadihrov ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@itmametskadihrov ~]$ ./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);
    [itmametskadihrov@itmametskadihrov ~]$ sudo chown root:guest /home/guest/readfile
    [itmametskadihrov@itmametskadihrov ~]$ sudo chmod u+s /home/guest/readfile
```

Рис. 3.13: Запуск программы readfile

3.2 Исследование Sticky-бита

Командой “ls -l / | grep tmp” убеждалась, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test командой “echo”test” > /tmp/file01.txt”. Просмотрела атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей “все остальные” командами “ls -l /tmp/file01.txt” и “chmod o+rw /tmp/file01.txt” (рис. 3.14).



```
itmametskadihrov@itmametskadihrov:~
[itmametskadihrov@itmametskadihrov ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 окт 6 18:42 tmp
[itmametskadihrov@itmametskadihrov ~]$
[guest@itmametskadihrov ~]$ echo "test" > /tmp/file01.txt
[guest@itmametskadihrov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт 6 17:55 /tmp/file01.txt
[guest@itmametskadihrov ~]$ chmod o+rw /tmp/file01.txt
[guest@itmametskadihrov ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт 6 17:55 /tmp/file01.txt
```

Рис. 3.14: Создание файла file01.txt

От имени пользователя guest2 попробовали прочитать файл командой “cat /tmp/file01.txt” - это удалось. Далее попытались дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой “chmod g+rw /tmp/file01.txt”. От имени пользователя guest2 попробовали удалить файл - это не удастся ни в каком из случаев, возникает ошибка (рис. 3.15).

```
[itmametskadihrov@itmametskadihrov ~]$ su - guest2
Пароль:
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'?
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

Рис. 3.15: Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

Повысили права до суперпользователя командой “su -” и выполнили команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинули режим суперпользователя командой “exit”. Повторили предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем (рис. 3.16).

```

[guest2@itmametskadihrov ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 окт 6 18:10 tmp
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test2" >> /tmp/file01.txt
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
test2
[guest2@itmametskadihrov ~]$ echo "test3" > /tmp/file01.txt
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test3
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
[guest2@itmametskadihrov ~]$

```

Рис. 3.16: Удаление атрибута t (Sticky-бита) и повторение действий

Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp (рис. 3.17).

```

itmametskadihrov@itma...
[itmametskadihrov@itmametskadihrov ~]$ su -
Пароль:
[root@itmametskadihrov ~]# chmod +t /tmp
[root@itmametskadihrov ~]# exit
ВЫХОД
[itmametskadihrov@itmametskadihrov ~]$
[guest2@itmametskadihrov ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 окт 6 18:50 tmp
[guest2@itmametskadihrov ~]$

```

Рис. 3.17: Возвращение атрибута t (Sticky-бита)

4 Выводы

В ходе выполнения данной лабораторной работы мы изучили механизмы изменения идентификаторов, применение SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

1. Стандартные права SetUID, SetGID, Sticky в Linux [Электронный ресурс].
URL: <https://linux-notes.org/standartny-e-prava-unix-suid-sgid-sticky-bity/>.