

Отчёт по лабораторной работе №5

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Подготовка к выполнению лабораторной работы	6
2.2	Выполнение лабораторной работы	7
2.2.1	Создание программы	7
2.2.2	Исследование Sticky-бита	12
3	Вывод	16
	Список литературы	17

Список иллюстраций

2.1	gcc -v	6
2.2	setenforce	6
2.3	компиляторы C и C++	7
2.4	Создание программы	7
2.5	Программа simpleid.c	8
2.6	Выполнение программы simpleid.c и id	8
2.7	Программа simpleid2.c	9
2.8	Запуск программы simpleid2.c	9
2.9	Установка атрибутов	9
2.10	Программа simpleid2.c и id	10
2.11	Создание программы readfile.c	10
2.12	Программа readfile.c	10
2.13	Компилирование программы readfile.c	11
2.14	Чтение файла readfile.c	11
2.15	Чтение файла readfile.c	11
2.16	Чтение файла /etc/shadow	12
2.17	Чтение файла simpleid2.c	12
2.18	Работа с файлом	13
2.19	Удаляем /tmp/file01.txt	13
2.20	Суперпользователь	14
2.21	Работа без атрибута t	14
2.22	Работа без атрибута t	15

Список таблиц

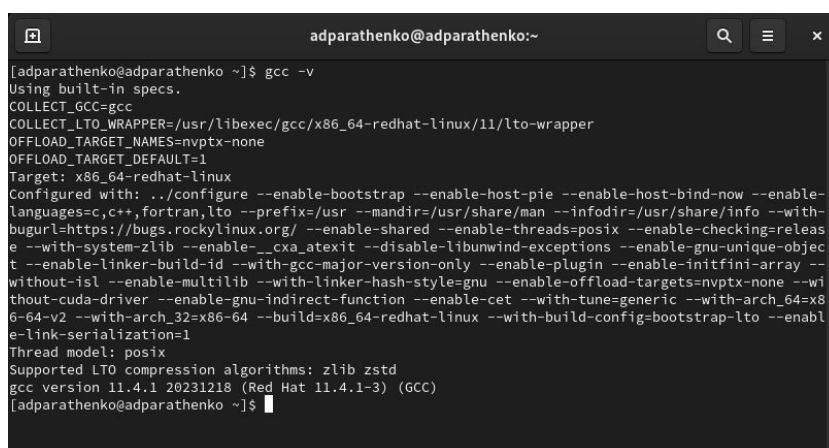
1 Цель работы

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 Выполнение лабораторной работы

2.1 Подготовка к выполнению лабораторной работы

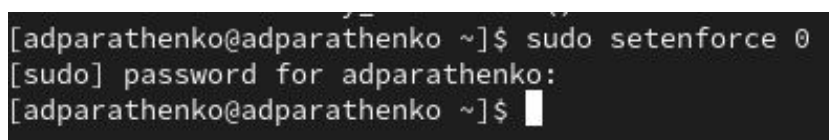
- 1) Проверяем установлен ли компилятор gcc командой `gcc -v` (рис. 2.1)



```
adparathenko@adparathenko:~$ gcc -v
Using built-in specs.
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
Target: x86_64-redhat-linux
Configured with: ../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-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_64=x86_64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-serialization=1
Thread model: posix
Supported LTO compression algorithms: zlib zstd
gcc version 11.4.1 20231218 (Red Hat 11.4.1-3) (GCC)
adparathenko@adparathenko:~$
```

Рис. 2.1: gcc -v

- 2) Отключаем систему запретов до очередной перезагрузки системы командой `setenforce 0` (рис. 2.2)



```
[adparathenko@adparathenko ~]$ sudo setenforce 0
[sudo] password for adparathenko:
[adparathenko@adparathenko ~]$
```

Рис. 2.2: setenforce

- 3) Проверяем наличие компиляторов C и C++ `whereis gcc whereis g++` (рис. 2.3)

```
[adparathenko@adparathenko ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.in
fo.gz
[adparathenko@adparathenko ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[adparathenko@adparathenko ~]$
```

Рис. 2.3: компиляторы С и С++

2.2 Выполнение лабораторной работы

2.2.1 Создание программы

- 1) Войдите в систему от имени пользователя guest.
- 2) Создайте программу simpleid.c (рис. 2.4) - (рис. 2.5)

```
Compilation terminated.
[quest@adparathenko ~]$ touch simpleid.c
[quest@adparathenko ~]$ ls
Desktop  5174  dir2  Documents  Downloads  Music  Pictures  Public  simpleid.c  Templates  Videos
[quest@adparathenko ~]$ gedit simpleid.c

(gedit:7194): dbind-WARNING **: 20:38:21.462: 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:7194): dconf-WARNING **: 20:38:21.800: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:21.808: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7194): dconf-WARNING **: 20:38:22.691: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:7194): WARNING **: 20:41:44.638: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7194): WARNING **: 20:41:44.631: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:7194): WARNING **: 20:41:46.215: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7194): WARNING **: 20:41:46.215: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

(gedit:7194): dconf-WARNING **: 20:41:46.961: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
[quest@adparathenko ~]$
```

Рис. 2.4: Создание программы



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

Рис. 2.5: Программа simpleid.c

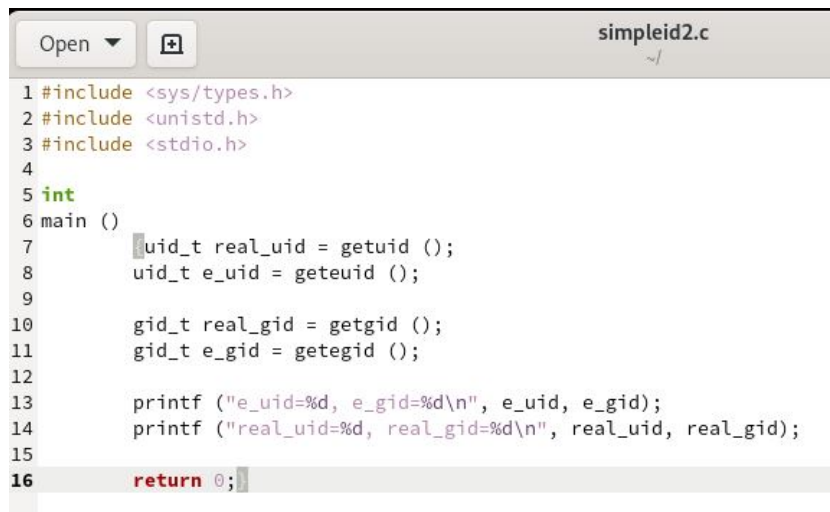
- 3) Скомпилировали программу и убедились, что файл программы создан **gcc simpleid.c -o simpleid**
- 4) Выполняем программу simpleid
- 5) Выполняем системную программу id и сравниваем результаты.(рис. 2.6)



```
[quest@adparathenko ~]$ gcc simpleid.c -o simpleid
[quest@adparathenko ~]$ ./simpleid
uid=1001, gid=1001
[quest@adparathenko ~]$ id
uid=1001(quest) gid=1001(quest) groups=1001(quest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[quest@adparathenko ~]$
```

Рис. 2.6: Выполнение программы simpleid.c и id

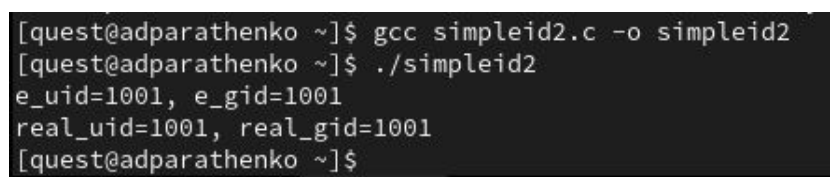
- 6) Усложняем программу, добавив вывод действительных идентификаторов. Получившуюся программу назовите simpleid2.c. (рис. 2.7)



```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int
6 main ()
7 {
8     uid_t real_uid = getuid ();
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     return 0;
17 }
```

Рис. 2.7: Программа simpleid2.c

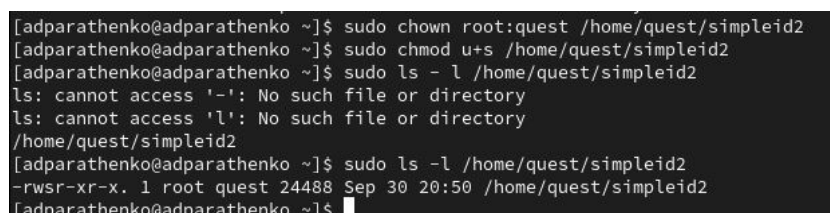
- 7) Компилируем и запускаем simpleid2.c: ***gcc simpleid2.c -o simpleid2***
./simpleid2 (рис. 2.8)



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

Рис. 2.8: Запуск программы simpleid2.c

- 8) От имени суперпользователя выполните команды: ***chown root:quest***
/home/guest/simpleid2 chmod u+s /home/guest/simpleid2
- 9) Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ***ls -l simpleid2*** (рис. 2.9)



```
[adparathenko@adparathenko ~]$ sudo chown root:quest /home/quest/simpleid2
[adparathenko@adparathenko ~]$ sudo chmod u+s /home/quest/simpleid2
[adparathenko@adparathenko ~]$ sudo ls -l /home/quest/simpleid2
ls: cannot access '-': No such file or directory
ls: cannot access 'l': No such file or directory
/home/quest/simpleid2
[adparathenko@adparathenko ~]$ sudo ls -l /home/quest/simpleid2
-rwsr-xr-x. 1 root quest 24488 Sep 30 20:50 /home/quest/simpleid2
[adparathenko@adparathenko ~]$
```

Рис. 2.9: Установка атрибутов

11) Запускаем simpleid2 и id: *./simpleid2 id* и сравниваем результаты. (рис. 2.10)

```
[quest@adparathenko ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[quest@adparathenko ~]$ id
uid=1001(quest) gid=1001(quest) groups=1001(quest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[quest@adparathenko ~]$
```

Рис. 2.10: Программа simpleid2.c и id

13) Создайте программу readfile.c: (рис. 2.11) - (рис. 2.12)

```
[quest@adparathenko ~]$ touch readfile.c
[quest@adparathenko ~]$ gedit readfile.c

(gedit:7622): dbind-WARNING **: 21:00:02.494: 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:7622): dconf-WARNING **: 21:00:02.501: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.600: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.844: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.845: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:7622): dconf-WARNING **: 21:00:02.849: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:7622): WARNING **: 21:05:19.120: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7622): WARNING **: 21:05:19.121: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

(gedit:7622): dconf-WARNING **: 21:05:22.096: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
```

Рис. 2.11: Создание программы readfile.c

Рис. 2.12: Программа readfile.c

- 14) Откомпилируем программу readfile.c. (рис. 2.13)

```
child process "dbus-launch" (No such file or directory)
[quest@adparathenko ~]$ gcc readfile.c -o readfile
[quest@adparathenko ~]$
```

Рис. 2.13: Компилирование программы readfile.c

- 15) Меняем владельца у файла readfile.c (или любого другого текстового файла в системе) и изменяем права так, чтобы только суперпользователь(root) мог прочитать его, а guest не мог.
- 16) Проверяем, что пользователь guest не может прочитать файл readfile.c (рис. 2.14)

```
[quest@adparathenko ~]$ cat readfile.c
cat: readfile.c: Permission denied
[quest@adparathenko ~]$
```

Рис. 2.14: Чтение файла readfile.c

- 17) Меняем у программы readfile владельца и установите SetU'D-бит.
- 18) Проверяем, может ли программа readfile прочитать файл readfile.c (рис. 2.15)

[illegible]

Рис. 2.15: Чтение файла readfile.c

19) Проверяем, может ли программа readfile прочитать файл /etc/shadow (рис. 2.16 - рис. 2.17)

[illegible]

Рис. 2.16: Чтение файла /etc/shadow

```
[quest@adparathenko ~]$ ./readfile 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;}
[quest@adparathenko ~]$ ./readfile readfile.c
```

Рис. 2.17: Чтение файла simpleid2.c

2.2.2 Исследование Sticky-бита

1) Выясним, установлен ли атрибут Sticky на директории /tmp командой **ls -l | grep tmp**

- 2) От имени пользователя `quest` создаём файл `file01.txt` в директории `/tmp` со словом `test`: **`echo "test" > /tmp/file01.txt`**
- 3) Просмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные»: **`ls -l /tmp/file01.txt`**
`chmod o+rw /tmp/file01.txt` **`ls -l /tmp/file01.txt`** (рис. 2.18)

```
[quest@adparathenko ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Sep 30 21:14 tmp
[quest@adparathenko ~]$ echo "test" > /tmp/file01.txt
[quest@adparathenko ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 quest quest 5 Sep 30 21:16 /tmp/file01.txt
[quest@adparathenko ~]$ chmod o+rw /tmp/file01.txt
chmod: invalid mode: 'o+rw'
Try 'chmod --help' for more information.
[quest@adparathenko ~]$ chmod o+rw /tmp/file01.txt
[quest@adparathenko ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 quest quest 5 Sep 30 21:16 /tmp/file01.txt
```

Рис. 2.18: Работа с файлом

4) От пользователя `quest2` (не являющегося владельцем) пробуем прочесть файл `/tmp/file01.txt`: **`cat /tmp/file01.txt`** 5) От пользователя `quest2` пробуем дописать в файл `/tmp/file01.txt` слово `test2` **`echo "test2" > /tmp/file01.txt`** 6) Проверяем содержимое файла **`cat /tmp/file01.txt`** 7) От пользователя `quest2` пробуем записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой **`echo "test3" > /tmp/file01.txt`** 8) Проверяем содержимое файла командой **`cat /tmp/file01.txt`** 9) От пользователя `quest2` пробуем удалить файл `/tmp/file01.txt` командой **`rm /tmp/file01.txt`** (рис. 2.19)

```
[quest@adparathenko ~]$ su - quest2
Password:
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test
[quest2@adparathenko ~]$ echo "test2" > /tmp/file01.txt
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test2
[quest2@adparathenko ~]$ echo "test3" > /tmp/file01.txt
[quest2@adparathenko ~]$ cat /tmp/file01.txt
test3
[quest2@adparathenko ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[quest2@adparathenko ~]$
```

Рис. 2.19: Удаляем `/tmp/file01.txt`

- 10) Повышаем свои права до суперпользователя следующей командой **su -** и выполняем после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: **chmod -t /tmp**
- 11) Покидаем режим суперпользователя командой **exit** (рис. 2.20)

```
password: get authentication tokens updated etc.
[adparathenko@adparathenko ~]$ su -
Password:
[root@adparathenko ~]# chmod -t /tmp
[root@adparathenko ~]# exit
logout
[adparathenko@adparathenko ~]$
```

Рис. 2.20: Суперпользователь

- 12) От пользователя guest2 проверяем, что атрибута t у директории /tmp нет: **ls -l / | grep tmp**
- 13) Повторяем предыдущие шаги. (рис. 2.21)

```
[adparathenko@adparathenko ~]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Sep 30 21:37 tmp
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test3
[adparathenko@adparathenko ~]$ echo "test2" >> /tmp/file01.txt
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test3
test2
[adparathenko@adparathenko ~]$ echo "test1" > /tmp/file01.txt
[adparathenko@adparathenko ~]$ cat /tmp/file01.txt
test1
[adparathenko@adparathenko ~]$ rm /tmp/file01.txt
```

Рис. 2.21: Работа без атрибута t

- 15) Повышаем свои права до суперпользователя и возвращаем атрибут t на директорию /tmp: **su - chmod +t /tmp exit** (рис. 2.22)

```
[adparathenko@adparathenko ~]$ su -  
Password:  
[root@adparathenko ~]# chmod +t /tmp  
[root@adparathenko ~]# exit  
logout  
[adparathenko@adparathenko ~]$ ls -l / | grep tmp  
drwxrwxrwt. 16 root root 4096 Sep 30 21:45 tmp  
[adparathenko@adparathenko ~]$
```

Рис. 2.22: Работа без атрибута t

3 Вывод

В результате выполнения работы я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

- 1) https://esystem.rudn.ru/pluginfile.php/2357153/mod_resource/content/2/005-lab_discret_sticky.pdf