Защита лабораторной работы №5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Смородова Дарья Владимировна 2022 Oct 8th

RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной

работы

Цель выполнения 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.

Результаты выполнения лабораторной работы

Проверка установки компилятора дсс

```
smorodovadv@smorodovadv ~1$ qcc -v
Используются внутренние спецификации.
COLLECT GCC=qcc
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 --enab
le-host-bind-now --enable-languages=c.c++.fortran.lto --prefix=/usr --mandir=/us
r/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/
 --enable-shared --enable-threads=posix --enable-checking=release --enable-multi
lib --with-system-zlib --enable- cxa atexit --disable-libunwind-exceptions --en
able-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --
with-linker-hash-style=gnu --enable-plugin --enable-initfini-array --without-is
 --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
Модель многопоточности: posix
Supported LTO compression algorithms: zlib zstd
gcc версия 11.2.1 20220127 (Red Hat 11.2.1-9) (GCC)
[smorodovadv@smorodovadv ~]$ yum install gcc
Ошибка: Эту команду нужно запускать с привилегиями суперпользователя (на большин
стве систем - под именем пользователя root).
[smorodovady@smorodovady ~1$ su
[root@smorodovadv smorodovadv]# vum install gcc
Последняя проверка окончания срока действия метаданных: 0:32:53 назад. Пт 30 сен
2022 17:20:18.
Пакет gcc-11.2.1-9.4.el9.x86 64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
```

Figure 1: Проверка установки компилятора gcc

Отключение системы запретов

```
[root@smorodovadv smorodovadv]# setenforce 0
[root@smorodovadv smorodovadv]# getenforce
Permissive
```

Figure 2: Отключение системы запретов

Проверка компиляторов

```
[root@smorodovadv smorodovadv]# whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /us
r/share/info/gcc.info.gz
[root@smorodovadv smorodovadv]# whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[root@smorodovadv smorodovadv]#
```

Figure 3: Проверка компиляторов

Содержимое файла 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;
```

Figure 4: Содержимое файла simpleid.c

Компиляция и запуск файла simpleid.c

```
[guest@smorodovadv ~]$ gcc simpleid.c -o simpleid
[guest@smorodovadv ~]$ ./simpleid
uid=1001, gid=1001
```

Figure 5: Компиляция и запуск файла simpleid.c

Команда id

```
[guest@smorodovadv ~]$ id
uid=1001[guest) gid=1001[guest) rpynnы=1001(guest) контекст=unconfined_u:unconfi
ned r:unconfined t:s0-s0:c0.c1023
[guest@smorodovadv ~]$ ■
```

Figure 6: Команда id

Содержимое файла simpleid2.c

```
1 #include <sys/types.h>
 2 #include <unistd.h>
 3 #include <stdio.h>
 5 int
 6 main()
 7
 8
          uid t real uid = getuid ();
          uid t e uid = geteuid ();
10
11
          gid t real gid = getgid ():
12
          gid t e gid = getegid ();
          printf ("e uid=%d, e gid=%d\n", e uid, e gid);
13
14
          printf ("real uid=%d, real gid=%d\n", real uid, real gid);
15
          return 0;
16
```

Figure 7: Содержимое файла simpleid2.c

Компиляция и запуск файла simpleid2.c

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

Figure 8: Компиляция и запуск файла simpleid2.c

Команды chown и chmod

```
[guest@smorodovadv ~]$ su
Пароль:
[root@smorodovadv guest]# chown root:guest /home/guest/simpleid2
[root@smorodovadv guest]# chmod u+s /home/guest/simpleid2
[root@smorodovadv guest]#
```

Figure 9: Команды chown и chmod

Проверка правильности установки новых атрибутов

```
[root@smorodovadv guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 сен 30 18:05 <mark>simpleid2</mark>
[root@smorodovadv guest]#
```

Figure 10: Проверка правильности установки новых атрибутов

Запуск simpleid2 и id

```
[root@smorodovadv guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@smorodovadv guest]# id
uid=0(root) gid=0(root) rpynnы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0-c0.1023
[root@smorodovadv guest]# ■
```

Figure 11: Запуск simpleid2 и id

Сравнение SetGID-бита

```
[root@smorodovady guest]# schaod g+s /home/guest/simpleid2
[root@smorodovady guest]# scisimpleid2
-rwsrwsr-x. 1 root guest 26008 ceн 30 18:05 simpleid2
[root@smorodovady guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@smorodovady guest]# id
uid=0[root] gid=0[root] rpynnы=0[root] контекст=unconfined_u:unconfined_r:unconfined_troot@smorodovady guest]# [
```

Figure 12: Сравнение SetGID-бита

Содержание файла readfile.c

```
1 #include <fcntl.h>
 2 #include <stdio.h>
 3 #include <sys/stat.h>
 4 #include <sys/types.h>
 5 #include <unistd.h>
 7 int
 8 main (int argc, char* argv[])
 9
10
          unsigned char buffer[16];
11
          size_t bytes read;
12
          int i:
13
14
           int fd = open (argv[1], 0 RDONLY);
15
           do
16
17
                  bytes read = read (fd, buffer, sizeof (buffer));
18
                  for (i = 0; i < bytes read; ++i) printf("%c", buffer[i]);
19
20
          while (bytes read == sizeof (buffer));
21
          close (fd):
22
           return Θ;
23
```

Figure 13: Содержание файла readfile.c

Компиляция файла readfile.c

```
[root@smorodovadv guest]# su guest
[guest@smorodovadv ~]$ touch readfile.c
[guest@smorodovadv ~]$ gcc readfile.c -o readfile
[guest@smorodovadv ~]$
```

Figure 14: Компиляция файла readfile.c

Смена владельца и прав у файла readfile.c

```
[guest@smorodovadv ~]$ su
Пароль:
[root@smorodovadv guest]# chown root:guest readfile.c
[root@smorodovadv guest]# chmod 700 readfile.c
```

Figure 15: Смена владельца и прав у файла readfile.c

Проверка возможности прочитать файл readfile.c

```
[root@smorodovadv guest]# su guest
[guest@smorodovadv ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@smorodovadv ~]$
```

Figure 16: Проверка возможности прочитать файл readfile.c

Смена у программы readfile владельца и установка SetU'D-бит

```
[guest@smorodovadv ~]$ su
Пароль:
[root@smorodovadv guest]# chown root:guest readfile.c
[root@smorodovadv guest]# chmod u+s readfile.c
[root@smorodovadv guest]#
```

Figure 17: Смена у программы readfile владельца и установка SetU'D-бит

Проверка возможности прочитать файл readfile.c

```
[root@smorodovadv guest]# ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
main (int argc, char* argv[])
        unsigned char buffer[16];
        size t bytes read;
        int i;
        int fd = open (argv[1], 0 RDONLY);
        do
                bytes read = read (fd, buffer, sizeof (buffer));
                for (\overline{i} = 0; i < bytes read; ++i) printf("%c", buffer[i]);
        while (bytes read == sizeof (buffer)):
        close (fd);
        return 0:
[root@smorodovadv guest]#
```

Figure 18: Проверка возможности прочитать файл readfile.c

Проверка возможности прочитать файл /etc/shadow

```
[root@smorodovadv guest]# ./readfile /etc/shadow
root:$6$MIUJDzjA/shK/XEE$FCafDmVfJ0Wm2UlrimsoOqph1F3qk947LxjFRTe/U4fezZ19Rho3CiH
avU4fL7ldPu8K0eD9vzIINhNJ630F2.::0:99999:7:::
bin:*:19123:0:99999:7:::
daemon:*:19123:0:99999:7:::
adm:*:19123:0:99999:7:::
lp:*:19123:0:99999:7:::
sync:*:19123:0:99999:7:::
shutdown:*:19123:0:99999:7:::
halt:*:19123:0:99999:7:::
mail:*:19123:0:99999:7:::
operator: *:19123:0:99999:7:::
games:*:19123:0:99999:7:::
ftp:*:19123:0:99999:7:::
nobody:*:19123:0:99999:7:::
systemd-coredump:!!:19245:::::
dbus:!!:19245:::::
polkitd:!!:19245:::::
rtkit:!!:19245:::::
sssd:!!:19245:::::
avahi:!!:19245:::::
pipewire:!!:19245:::::
libstoragemgmt:!!:19245:::::
tss:!!:19245:::::
geoclue:!!:19245:::::
cockpit-ws:!!:19245:::::
cockpit-wsinstance:!!:19245:::::
setroubleshoot:!!:19245:::::
flatpak:!!:19245:::::
colord:!!:19245:::::
```

Figure 19: Проверка возможности прочитать файл /etc/shadow

Проверка установки атрибута Sticky на директории /tmp

```
[root@smorodovadv guest]# ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 сен 30 19:03 <mark>tmp</mark>
[root@smorodovadv guest]#
```

Figure 20: Проверка установки атрибута Sticky на директории /tmp

Создание файла fileO1.txt в директории /tmp со словом test

```
[guest@smorodovadv~]$ echo "test" > /tmp/file01.txt
[guest@smorodovadv ~]$
```

Figure 21: Создание файла file01.txt в директории /tmp со словом test

Просмотр атрибутов и разрешение чтения и записи для категории пользователей «все остальные»

```
[guest@smorodovadv ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ceH 30 19:06 /tmp/file01.txt
[guest@smorodovadv ~]$ chmod o+rw /tmp/file01.txt
[guest@smorodovadv ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ceH 30 19:06 /tmp/file01.txt
[guest@smorodovadv ~]$ |
```

Figure 22: Просмотр атрибутов и разрешение чтения и записи для категории пользователей «все остальные»

Попытка прочитать файл /tmp/file01.txt от пользователя guest2

```
[guest@smorodovadv ~]$ su
Пароль:
[root@smorodovadv guest]# su guest2
[guest2@smorodovadv guest]$ cat /tmp/file01.txt
test
[guest2@smorodovadv guest]$
```

Figure 23: Попытка прочитать файл /tmp/file01.txt от пользователя guest2

Попытка дозаписать в файл /tmp/file01.txt слово test2 от пользователя guest2

```
[guest2@smorodovadv guest]$ echo "test2">> /tmp/file01.txt
[guest2@smorodovadv guest]$ cat /tmp/file01.txt
test
test2
[guest2@smorodovadv guest]$
```

Figure 24: Попытка дозаписать в файл /tmp/file01.txt слово test2 от пользователя guest2

Попытка перезаписать файл /tmp/file01.txt словом test3 от пользователя guest2

```
[guest2@smorodovadv guest]$ echo "test3"> /tmp/file01.txt
[guest2@smorodovadv guest]$ cat /tmp/file01.txt
test3
[quest2@smorodovadv quest]$
```

Figure 25: Попытка перезаписать файл /tmp/file01.txt словом test3 от пользователя guest2

Попытка удалить файл /tmp/file01.txt от пользователя guest2

```
[guest2@smorodovadv guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@smorodovadv guest]$
```

Figure 26: Попытка удалить файл /tmp/file01.txt от пользователя guest2

Снятие атрибута t с директории /tmp

```
[guest2@smorodovadv guest]$ su -
Пароль:
[root@smorodovadv ~]# chmod -t /tmp
[root@smorodovadv ~]# exit
выход
[guest2@smorodovadv guest]$
```

Figure 27: Снятие атрибута t с директории /tmp

Проверка снятия атрибута t с директории /tmp

```
[guest2@smorodovadv guest]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 сен 30 19:14 <mark>tmp</mark>
[guest2@smorodovadv guest]$
```

Figure 28: Проверка снятия атрибута t с директории /tmp

Повтор предыдущих шагов

```
[guest2@smorodovadv guest]$ echo "test" > /tmp/file01.txt
[guest2@smorodovadv guest]$ echo "test2">> /tmp/file01.txt
[guest2@smorodovadv guest]$ cat /tmp/file01.txt
test2
[guest2@smorodovadv guest]$ echo "test3"> /tmp/file01.txt
[guest2@smorodovadv guest]$ cat /tmp/file01.txt
test3
[guest2@smorodovadv guest]$ rm /tmp/file01.txt
[guest2@smorodovadv guest]$ rm /tmp/file01.txt
```

Figure 29: Повтор предыдущих шагов

Возвращение атрибута t директории /tmp

```
[guest2@smorodovadv guest]$ su -
Пароль:
[root@smorodovadv ~]# chmod +t /tmp
[root@smorodovadv ~]# exit
выход
[guest2@smorodovadv guest]$
```

Figure 30: Возвращение атрибута t директории /tmp



- · Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов;
- Получили практические навыки работы в консоли с дополнительными атрибутами;
- Рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.