Лабораторная работа №6

Ilyinsky A. Arseniy

RUDN University, 2022 Moscow, Russia

Мандатное разграничение прав в Linux

Цель выполнения 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 работы

Выполнение работы

```
[arilinskiy@arilinskiy ~]$ 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/ --enab
le-shared --enable-threads=posix --enable-checking=release --enable-multilib --w
ith-system-zlib --enable-__cxa_atexit --disable-libunwind-exceptions --enable-gn
u-unique-object --enable-linker-build-id --with-gcc-major-version-only --with-li
nker-hash-style=gnu --enable-plugin --enable-initfini-array --without-isl --enab
le-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-functi
on --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-s
erialization=1
Thread model: posix
Supported LTO compression algorithms: zlib zstd
gcc version 11.2.1 20220127 (Red Hat 11.2.1-9) (GCC)
[arilinskiy@arilinskiy ~]$
```

Рис.1 Компилятор gcc

Выполнение работы

```
[guest@arilinskiy ~]$ su
Password:
[root@arilinskiy guest]# setenforce 0
[root@arilinskiy guest]# getenforce 0
Permissive
[root@arilinskiy guest]#
```

Рис.2 Отключение SELinux

Выполнение работы

```
[guest@arilinskiy ~]$ touch simpleid.c
[guest@arilinskiy ~]$ ls
Desktop  Documents  Music     Public      Templates
dir1     Downloads  Pictures  simpleid.c  Videos
[guest@arilinskiy ~]$ vim simpleid.c
```

Рис.3 Создание программы simpleid.c

Выполнение работы

```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;
}
```

Код программы simpleid.c

Выполнение работы

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

Рис.4 Компиляция и выполнение simpleid.c

Выполнение работы

```
[guest@arilinskiy ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

Рис.5 Результат команды id

Выполнение работы

```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;
}
```

Код программы simpleid2.c

Выполнение работы

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

Рис.6 Компиляция и выполнение simpleid2

Выполнение работы

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

```
[guest@arilinskiy ~]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 26008 Oct  6 14:02 simpleid2
```

Рис.7 Изменение владельца и прав на файл simpleid2

Выполнение работы

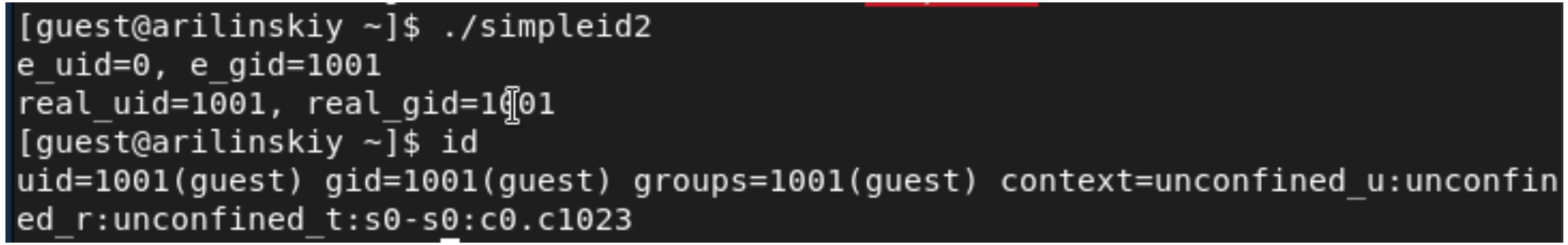

Рис.8 Выполнение simpleid2 и id

Выполнение работы

```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);
        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;
}
```

Код программы readfile.c

Выполнение работы

```
[guest@arilinskiy ~]$ gcc readfile.c -o readfile
[guest@arilinskiy ~]$ su
Password:
[root@arilinskiy guest]# chown root:guest /home/guest/readfile.c
[root@arilinskiy guest]# chmod 700 /home/guest/readfile.c
[root@arilinskiy guest]#
exit
[guest@arilinskiy ~]$ ls -l readfile.c
-rwx------. 1 root guest 415 Oct  6 14:14 readfile.c
[guest@arilinskiy ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Рис.9 Изменение владельца и прав на файл readfile.c. Получение отказа в чтении подьзователю guest

Выполнение работы

```
[guest@arilinskiy ~]$ su
Password:
[root@arilinskiy guest]# chown root:guest /home/guest/readfile
[root@arilinskiy guest]# chmod u+s /home/guest/readfile
```

Рис.11 Установка UID бита для readfile.c

Выполнение работы

```
[guest@arilinskiy ~]$ ./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);
        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;
}
```

Рис.12 Выполнение программы для файла readfile.c

Выполнение работы

```
[guest@arilinskiy ~]$ ./readfile /etc/shadow
root:$6$gVF5yHxGxqk9gOoX$iVHgsVLtBcp/ewkZGke73j4AmCU5/X05S0VimcXIz9sgfGJ347wqXdU
a2jwUqru6Tiiq0PK0zHZFaijTmC7ET.::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:!!:19244::::::
dbus:!!:19244::::::
polkitd:!!:19244::::::
rtkit:!!:19244::::::
```

Рис.13 Выполнение программы для файла /etc/shadow

Выполнение работы

```
[guest@arilinskiy ~]$ ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 Oct  6 14:20 tmp
[guest@arilinskiy ~]$ echo "test" > /tmp/file01.txt
[guest@arilinskiy ~]$ cat /tmp/file01.txt
test
[guest@arilinskiy ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  6 14:24 /tmp/file01.txt
[guest@arilinskiy ~]$ chmod o+rw /tmp/file01.txt
[guest@arilinskiy ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  6 14:24 /tmp/file01.txt
[guest@arilinskiy ~]$ su guest2
Password:
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test
[guest2@arilinskiy guest]$ echo "test2" >> /tmp/file01.txt
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test
test2
[guest2@arilinskiy guest]$ echo "test3" > /tmp/file01.txt
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test3
[guest2@arilinskiy guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@arilinskiy guest]$
```

Рис.14 Работа со Sticky битом

Выполнение работы

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

Рис.15 Работа с файлом без Sticly бита (1/2)

Выполнение работы

```
[guest2@arilinskiy guest]$ ls -l / | grep tmp
drwxrwxrwx.  16 root root 4096 Oct  6 14:29 tmp
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test3
[guest2@arilinskiy guest]$ echo "test2" >> /tmp/file01.txt
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test3
test2
[guest2@arilinskiy guest]$ echo "test3" > /tmp/file01.txt
[guest2@arilinskiy guest]$ cat /tmp/file01.txt
test3
[guest2@arilinskiy guest]$ rm /tmp/file01.txt
[guest2@arilinskiy guest]$ ls /tmp
dbus-NLvZQkBZqo
dbus-QFSlYBR8sf
dbus-rbWiPQWEme
systemd-private-017df871978e423a82ee6ca025d81135-chronyd.service-aAgCqB
systemd-private-017df871978e423a82ee6ca025d81135-colord.service-gqetFK
systemd-private-017df871978e423a82ee6ca025d81135-dbus-broker.service-oqrQ9M
systemd-private-017df871978e423a82ee6ca025d81135-fwupd.service-0w4xdc
systemd-private-017df871978e423a82ee6ca025d81135-ModemManager.service-plAcsf
systemd-private-017df871978e423a82ee6ca025d81135-power-profiles-daemon.service-8
UrqWX
systemd-private-017df871978e423a82ee6ca025d81135-rtkit-daemon.service-MhmQI1
systemd-private-017df871978e423a82ee6ca025d81135-switcheroo-control.service-Gz3Y
Uy
systemd-private-017df871978e423a82ee6ca025d81135-systemd-logind.service-BZIHnI
systemd-private-017df871978e423a82ee6ca025d81135-upower.service-iuE72k
```

Рис.15 Работа с файлом без Sticly бита (2/2)

Выполнение работы

```
[guest2@arilinskiy guest]$ su
Password:
[root@arilinskiy guest]# chmod +t /tmp
[root@arilinskiy guest]# ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 Oct  6 14:34 tmp
[root@arilinskiy guest]#
exit
[guest2@arilinskiy guest]$
```

Рис.16 Установление атрибута t

Вывод

Спасибо за внимание