

```
## Front matter
lang: ru-RU title:
Лабораторная
работа №5
subtitle:
Дискреционное
разграничение
прав в Linux.
Исследование
влияния
дополнительных
атрибутов
author: -
Камкина А. Л.
institute: -
Российский
университет
дружбы
народов, Москва,
Россия
## i18n babel
babel-lang:
russian babel-
otherlangs:
english
## Formatting
pdf toc: false toc-
title: Содержание
slide_level: 2
aspectratio: 169
section-titles: true
theme:
metropolis
header-includes: -
- " " - "
```

Информация

Докладчик

- Камкина Арина Леонидовна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- 1032216456@pfur.ru

- <https://alkamkina.github.io/ru/>



Вводная часть

Цели и задачи

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.

Задачи:

- Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов
- Просмотр влияние бита Sticky на запись и удаление файлов

Инструмент: VirtualBox - CentOS, cmd

Выполнение лабораторной работы

Проверили установлен ли компилятор gcc - установлен

```
[alkamkina@alkamkina ~]$ 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++,f
ortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=http://bugzilla.redhat.com/bugzill
a --enable-shared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libun
wind-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-c
uda-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 11.5.0 20240719 (Red Hat 11.5.0-2) (GCC)
```

#fig:001 width=70% }

Работа с simpleid.c

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

{ #fig:002 width=70% }

Текст программы simpleid.c

```
[alkamkina@alkamkina lab5]$ ls
presentation report
[alkamkina@alkamkina lab5]$ touch simpleid.c
[alkamkina@alkamkina lab5]$ ls
presentation report simpleid.c
[alkamkina@alkamkina lab5]$ gcc simpleid.c -o simpleid
[alkamkina@alkamkina lab5]$ ./simpleid
bash: ./simpleid: Нет такого файла или каталога
[alkamkina@alkamkina lab5]$ ./simpleid
uid=1000, gid=1000
[alkamkina@alkamkina lab5]$ id
uid=1000(alkamkina) gid=1000(alkamkina) группы=1000(alkamkina) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

#fig:003 width=70% }

Работа с simpleid2.c

```
[alkamkina@alkamkina lab5]$ ls
presentation report
[alkamkina@alkamkina lab5]$ touch simpleid.c
[alkamkina@alkamkina lab5]$ ls
presentation report simpleid.c
[alkamkina@alkamkina lab5]$ gcc simpleid.c -o simpleid
[alkamkina@alkamkina lab5]$ ./simpleid
bash: ./simpleid: Нет такого файла или каталога
[alkamkina@alkamkina lab5]$ ./simpleid
uid=1000, gid=1000
[alkamkina@alkamkina lab5]$ id
uid=1000(alkamkina) gid=1000(alkamkina) группы=1000(alkamkina) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

#fig:003 width=70% }

Компиляция и запуск simpleid2.c

```
[alkamkina@alkamkina lab5]$ gcc simpleid2.c -o simpleid2
[alkamkina@alkamkina lab5]$ ./simpleid2
e_uid=1000, e_gid=1000
real_uid=1000, real_gid=1000
```

{ #fig:005 width=70%

Работа с атрибутами

```
[root@alkamkina lab5]# chown root:alkamkina simpleid2
[root@alkamkina lab5]# chmod u+s simpleid2
[root@alkamkina lab5]# ls -l simpleid2
-rwsr-xr-x. 1 root alkamkina 17656 окт  4 18:04 simpleid2
[root@alkamkina lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@alkamkina lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

#fig:006 width=70% }

Создание readfile.c

```
[root@alkamkina lab5]# touch readfile.c
[root@alkamkina lab5]# chmod 777 readfile.c
[root@alkamkina lab5]# gcc readfile.c -o readfile
```

{ #fig:007 width=70% }

8. Текст программы readfile.c

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

#fig:008 width=70% }

Просмотр файла readfile.c

```
[root@alkamkina lab5]# chown root:alkamkina readfile.c
[root@alkamkina lab5]# chmod 700 readfile.c
[root@alkamkina lab5]# cat 700 readfile.c
cat: 700: Нет такого файла или каталога
#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;
}

[root@alkamkina lab5]# exit
выход
[alkamkina@alkamkina lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
```

#fig:009 width=70% }

Исследование Sticky-бита


```

[alkamkina@alkamkina ~]$ cd /tmp
[alkamkina@alkamkina tmp]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 окт  4 18:23 tmp
[alkamkina@alkamkina tmp]$ echo "test" > /tmp/file01.txt
[alkamkina@alkamkina tmp]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 alkamkina alkamkina 5 окт  4 18:29 /tmp/file01.txt
[alkamkina@alkamkina tmp]$ chmod o+r /tmp/file01.txt
[alkamkina@alkamkina tmp]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 alkamkina alkamkina 5 окт  4 18:29 /tmp/file01.txt
[alkamkina@alkamkina tmp]$ su - guest3
Пароль:
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test
[guest3@alkamkina ~]$ echo "test2" > /tmp/file01.txt
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test2
[guest3@alkamkina ~]$ echo "test2" >> /tmp/file01.txt
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test2
test2
[guest3@alkamkina ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Нет такого файла или каталога
[guest3@alkamkina ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Нет такого файла или каталога
[guest3@alkamkina ~]$ ls tmp
ls: невозможно получить доступ к 'tmp': Нет такого файла или каталога
[guest3@alkamkina ~]$ cd tmp
-bash: cd: tmp: Нет такого файла или каталога
[guest3@alkamkina ~]$ su -
Пароль:
su: Сбой при проверке подлинности
[guest3@alkamkina ~]$ su -
Пароль:
[root@alkamkina ~]# chmod -t /tmp
[root@alkamkina ~]# exit
выход
[guest3@alkamkina ~]$ ls -l / | grep tmp
drwxrwxrwx. 19 root root 4096 окт  4 18:34 tmp
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test2
test2
[guest3@alkamkina ~]$ echo "test3" >> /tmp/file01.txt
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test2
test2
test3
[guest3@alkamkina ~]$ echo "test4" > /tmp/file01.txt
[guest3@alkamkina ~]$ cat /tmp/file01.txt
test4
[guest3@alkamkina ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Нет такого файла или каталога
[guest3@alkamkina ~]$ rm /tmp/file01.txt
[guest3@alkamkina ~]$ ls tmp
ls: невозможно получить доступ к 'tmp': Нет такого файла или каталога
[guest3@alkamkina ~]$ ls /tmp
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-chrond.service-cSHoNP
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-colord.service-q5xn9X
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-dbus-broker.service-AWu3cp
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-fwupd.service-Ex40RF
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-kdump.service-ycvEUz
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-ModemManager.service-X9SjVU
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-power-profiles-daemon.service-cVI1b4
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-rtkit-daemon.service-9vJmBX
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-switcheroo-control.service-QzV
Hhb
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-systemd-logind.service-rKXi7N
systemd-private-3d308cdb2ace4f22b00835db8b43fd81-upower.service-fil2hH
Temp-5b8f27d5-0d9d-4517-9f68-3b5d1c695393
[guest3@alkamkina ~]$ su -
Пароль:
[root@alkamkina ~]# chmod +t /tmp
[root@alkamkina ~]# exit

```

{ #fig:010

```
width=70% }
```

Заключение

Вывод

В результате выполнения работы я изучила механизмы изменения идентификаторов и применения SetUID- и Sticky-битов