

Основы информационной безопасности. Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Нзита Диатезилуа Катенди

05 октября 2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- <https://github.com/NzitaKatendi>

Вводная часть

Целью данной работы является 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.

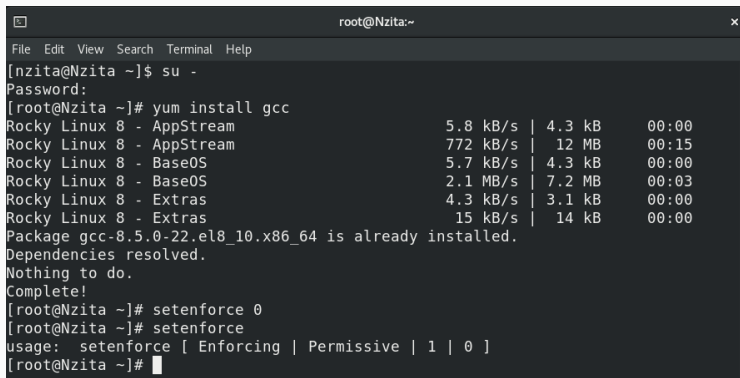
Задачи:

- Изменение идентификаторов и применение SetUID- и Sticky-битов
- Проверка прав доступа при разных дополнительных атрибутах

Инструмент VirtualBox, bash


Выполнение лабораторной работы

Подготовка лабораторного стенда



```
root@Nzita:~  
File Edit View Search Terminal Help  
[nzita@Nzita ~]$ su -  
Password:  
[root@Nzita ~]# yum install gcc  
Rocky Linux 8 - AppStream          5.8 kB/s | 4.3 kB      00:00  
Rocky Linux 8 - AppStream          772 kB/s | 12 MB      00:15  
Rocky Linux 8 - BaseOS             5.7 kB/s | 4.3 kB      00:00  
Rocky Linux 8 - BaseOS             2.1 MB/s | 7.2 MB      00:03  
Rocky Linux 8 - Extras             4.3 kB/s | 3.1 kB      00:00  
Rocky Linux 8 - Extras             15 kB/s | 14 kB      00:00  
Package gcc-8.5.0-22.el8_10.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@Nzita ~]# setenforce 0  
[root@Nzita ~]# setenforce  
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]  
[root@Nzita ~]#
```

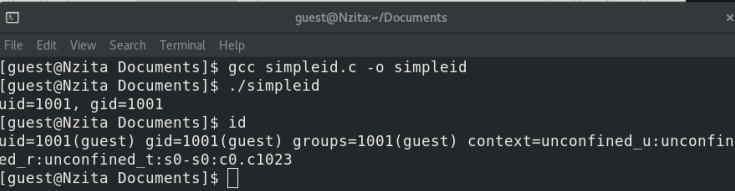
Рис. 1: Подготовка лабораторного стенда



```
*simpleid.c
~/Documents

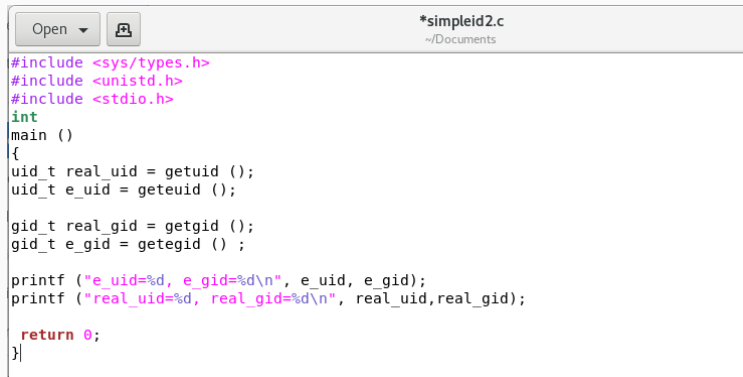
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Рис. 2: Текст программы simpleid.c



```
guest@Nzita:~/Documents
File Edit View Search Terminal Help
[guest@Nzita Documents]$ gcc simpleid.c -o simpleid
[guest@Nzita Documents]$ ./simpleid
uid=1001, gid=1001
[guest@Nzita Documents]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@Nzita Documents]$
```

Рис. 3: Запуск программы simpleid



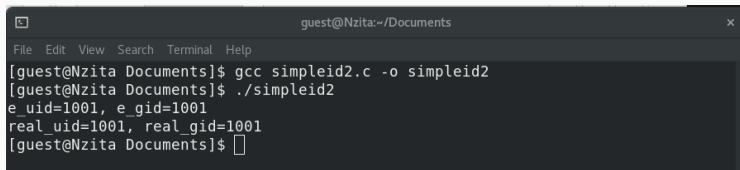
```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
    uid_t real_uid = getuid ();
    uid_t e_uid = geteuid ();

    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;
}
```

Рис. 4: Текст программы simpleid2.c



```
guest@Nzita:~/Documents
File Edit View Search Terminal Help
[guest@Nzita Documents]$ gcc simpleid2.c -o simpleid2
[guest@Nzita Documents]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@Nzita Documents]$
```

Рис. 5: Запуск программы simpleid2

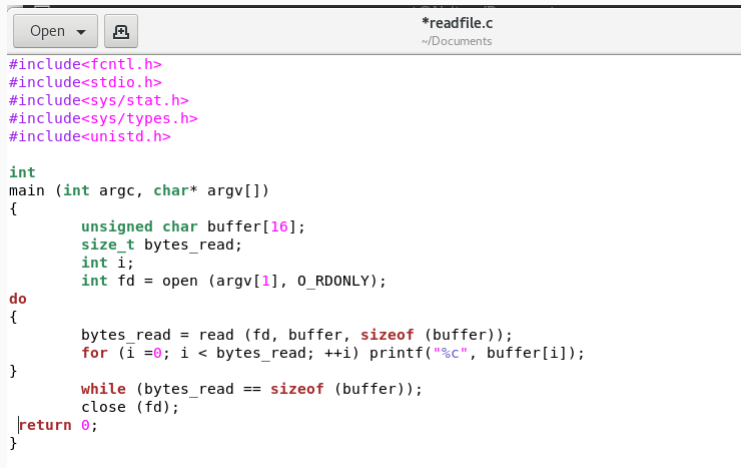
Изменение и проверка прав доступа

```
[root@Nzita ~]# chown root:guest /home/guest/Documents/simpleid2
[root@Nzita ~]# chown root:guest /home/guest/Documents/simpleid2
[root@Nzita ~]# ls -l /home/guest/Documents/simpleid2
-rwxrwxr-x. 1 root guest 18312 Oct  2 13:34 /home/guest/Documents/simpleid2
[root@Nzita ~]# exit
logout
[nzita@Nzita ~]$ su - guest
Password:
[guest@Nzita ~]$ cd Documents/
[guest@Nzita Documents]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@Nzita Documents]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfine
d_r:unconfined_t:s0-s0:c0.c1023
[guest@Nzita Documents]$ su - Nzita
su: user Nzita does not exist
[guest@Nzita Documents]$ su - nzita
Password:
[nzita@Nzita ~]$ su -
Password:
[root@Nzita ~]# /home/guest/Documents/simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@Nzita ~]#
```

Рис. 6: Изменение владельца и запуск программы simpleid2 с установленным SetUID-битом

```
[root@Nzita ~]# chmod u-s /home/guest/Documents/simpleid2
[root@Nzita ~]# chmod u+g /home/guest/Documents/simpleid2
[root@Nzita ~]# exit
logout
[nzita@Nzita ~]$ ls -l simpleid2
ls: cannot access 'simpleid2': No such file or directory
[nzita@Nzita ~]$ su - guest
Password:
[guest@Nzita ~]$ cd Documents
[guest@Nzita Documents]$ ls -l simpleid2
-rwxrwxr-x. 1 root guest 18312 Oct  2 13:34 simpleid2
[guest@Nzita Documents]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@Nzita Documents]$
```

Рис. 7: Запуск программы simpleid2 с установленным SetGID-битом



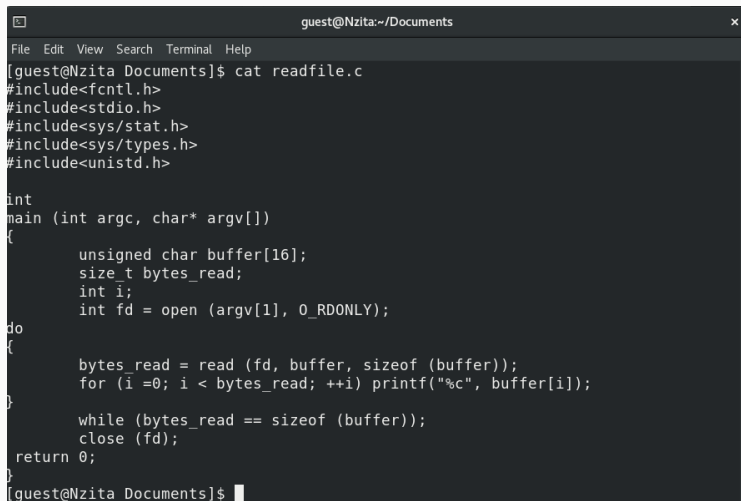
```
#include<fcntl.h>
#include<stdio.h>
#include<sys/stat.h>
#include<sys/types.h>
#include<unistd.h>

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. 8: Текст программы readfile.c

Изменение и проверка прав доступа

A terminal window titled 'guest@Nzita:~/Documents' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'cat readfile.c' and the following C code:

```
[guest@Nzita Documents]$ cat 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;
[guest@Nzita Documents]$
```

Рис. 9: Изменение владельца и прав файла readfile.c

Изменение и проверка прав доступа

```
[guest@Nzita Documents]$ ls -l / | grep tmp
drwxrwxrwt. 14 root root 4096 Oct  2 14:00 tmp
[guest@Nzita Documents]$ echo "test" > /tmp/file01.txt
[guest@Nzita Documents]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  2 14:04 /tmp/file01.txt
[guest@Nzita Documents]$ chmod o+rw /tmp/file01.txt
[guest@Nzita Documents]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  2 14:04 /tmp/file01.txt
[guest@Nzita Documents]$ su - guest2
Password:
[guest2@Nzita ~]$ cat /tmp/file01.txt
test
[guest2@Nzita ~]$ echo "test2" > /tmp/file01.txt
[guest2@Nzita ~]$ cat /tmp/file01.txt
test2
[guest2@Nzita ~]$ echo "test3" > /tmp/file01.txt
[guest2@Nzita ~]$ cat /tmp/file01.txt
test3
[guest2@Nzita ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@Nzita ~]$ su -
Password:
[root@Nzita ~]# chmod -t /tmp
[root@Nzita ~]# exit
logout
[guest2@Nzita ~]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 Oct  2 14:10 tmp
[guest2@Nzita ~]$ cat /tmp/file01/txt
cat: /tmp/file01/txt: No such file or directory
[guest2@Nzita ~]$ cat /tmp/file01.txt
test3
[guest2@Nzita ~]$ echo "test3" > /tmp/file01.txt
[guest2@Nzita ~]$ cat /tmp/file01.txt
test3
[guest2@Nzita ~]$ rm /tmp/file01.txt
[guest2@Nzita ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```


Заключение

В результате выполнения работы были выполнены:

- 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.

1. Граннеман С. Скотт Граннеман: Linux. Карманный справочник. 2-е изд. Вильямс, 2019. 464 с.