

Основы информационной безопасности. Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Демидова Е.А.

09.09.2023

Российский Университет дружбы народов

Информация

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/eademidova>



Вводная часть

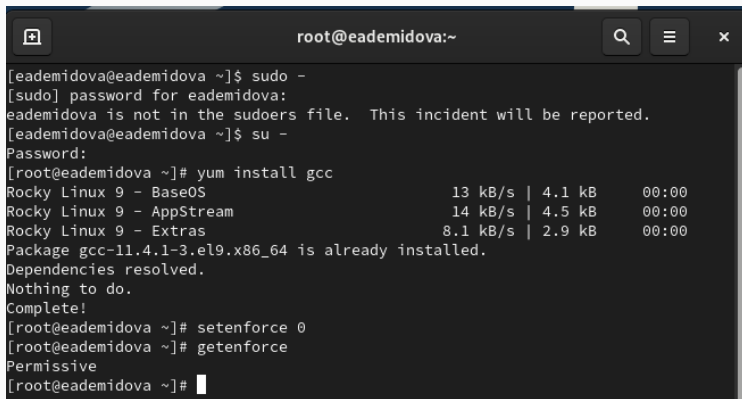
Целью данной работы является изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Задачи:

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

Инструмент: VirtualBox, bash

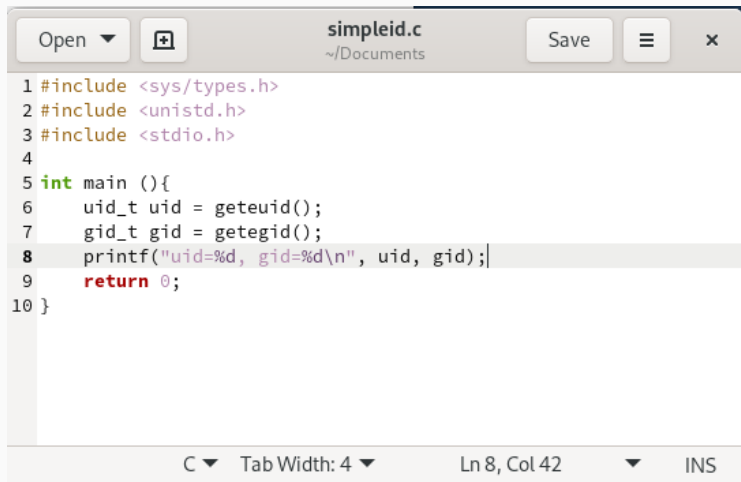
Выполнение лабораторной работы



A terminal window titled 'root@eademidova:~' with search, menu, and close buttons. The terminal shows the following commands and output:

```
[eademidova@eademidova ~]$ sudo -  
[sudo] password for eademidova:  
eademidova is not in the sudoers file. This incident will be reported.  
[eademidova@eademidova ~]$ su -  
Password:  
[root@eademidova ~]# yum install gcc  
Rocky Linux 9 - BaseOS                13 kB/s | 4.1 kB    00:00  
Rocky Linux 9 - AppStream              14 kB/s | 4.5 kB    00:00  
Rocky Linux 9 - Extras                 8.1 kB/s | 2.9 kB    00:00  
Package gcc-11.4.1-3.el9.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@eademidova ~]# setenforce 0  
[root@eademidova ~]# getenforce  
Permissive  
[root@eademidova ~]#
```

Рис. 1: Подготовка лабораторного стенда



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

C ▾ Tab Width: 4 ▾ Ln 8, Col 42 ▾ INS

Рис. 2: Текст программы simpleid.c


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

Рис. 3: Запуск программы simpleid



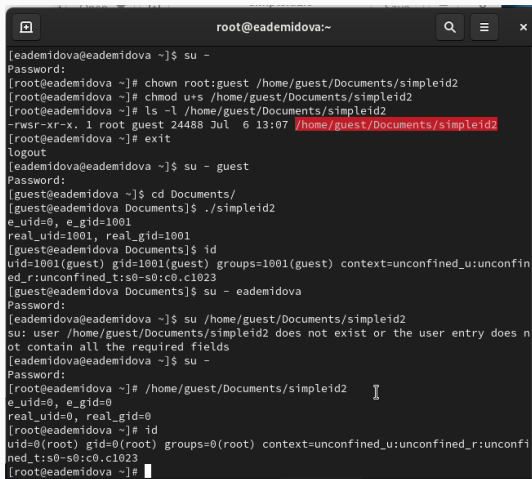
```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int main ()
6     uid_t real_uid = getuid();
7     uid_t e_uid = geteuid();
8
9     gid_t real_gid = getgid();
10    gid_t e_gid = getegid();
11
12    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
13    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
14    return 0;
15
```

Рис. 4: Текст программы simpleid2.c

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

Рис. 5: Запуск программы simpleid2

Изменение и проверка прав доступа



```
root@eademidova:~  
[eademidova@eademidova ~]$ su -  
Password:  
[root@eademidova ~]# chown root:guest /home/guest/Documents/simpleid2  
[root@eademidova ~]# chmod u+s /home/guest/Documents/simpleid2  
[root@eademidova ~]# ls -l /home/guest/Documents/simpleid2  
-rwsr-xr-x. 1 root guest 24488 Jul  6 13:07 /home/guest/Documents/simpleid2  
[root@eademidova ~]# exit  
logout  
[eademidova@eademidova ~]$ su - guest  
Password:  
[guest@eademidova ~]$ cd Documents/  
[guest@eademidova Documents]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@eademidova Documents]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@eademidova Documents]$ su - eademidova  
Password:  
[eademidova@eademidova ~]$ su /home/guest/Documents/simpleid2  
su: user /home/guest/Documents/simpleid2 does not exist or the user entry does not contain all the required fields  
[eademidova@eademidova ~]$ su -  
Password:  
[root@eademidova ~]# /home/guest/Documents/simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@eademidova ~]# id  
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@eademidova ~]#
```

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

Изменение и проверка прав доступа

```
[guest@eademidova Documents]$ su -  
Password:  
[root@eademidova ~]# chmod u-s /home/guest/Documents/simpleid2  
[root@eademidova ~]# chmod g+s /home/guest/Documents/simpleid2  
[root@eademidova ~]# exit  
logout  
[guest@eademidova Documents]$ ls -l simpleid2  
-rwxr-sr-x. 1 root guest 24488 Jul 6 13:07 simpleid2  
[guest@eademidova Documents]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@eademidova Documents]$ ud  
bash: ud: command not found...  
Similar command is: 'du'  
[guest@eademidova Documents]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@eademidova Documents]$
```

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

```
GNU nano 5.6.1 /home/guest/Documents/readfile.c
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>

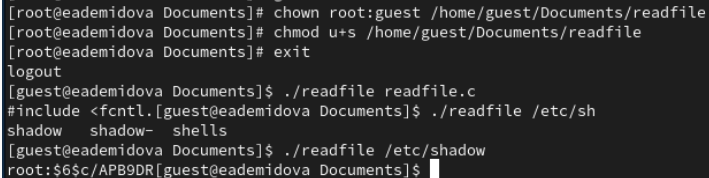
int main(int argc, char* argv[]){
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    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

```
guest@eademidova:~$  
[guest@eademidova Documents]$ gcc readfile.c -o readfile  
[guest@eademidova Documents]$ ./readfile  
[guest@eademidova Documents]$ cat readfile.c  
#include <sys/types.h>  
#include <sys/stat.h>  
#include <fcntl.h>  
#include <unistd.h>  
#include <stdio.h>  
  
int main(int argc, char* argv[]){  
    unsigned char buffer[16];  
    size_t bytes_read;  
    int i;  
  
    int fd = open(argv[1], O_RDONLY);  
    close(fd);  
    return 0;  
}  
[guest@eademidova Documents]$ su -  
Password:  
[root@eademidova ~]# chown root:guest /home/guest/Documents/readfile.c  
[root@eademidova ~]# chmod 700 /home/guest/Documents/readfile.c  
[root@eademidova ~]# cat /home/guest/Documents/readfile.c  
#include <sys/types.h>  
#include <sys/stat.h>  
#include <fcntl.h>  
#include <unistd.h>  
#include <stdio.h>  
  
int main(int argc, char* argv[]){  
    unsigned char buffer[16];  
    size_t bytes_read;  
    int i;  
  
    int fd = open(argv[1], O_RDONLY);  
    close(fd);  
    return 0;  
}  
[root@eademidova ~]# exit  
logout  
[guest@eademidova Documents]$ cat readfile.c  
cat: readfile.c: Permission denied
```



```
[root@eademidova Documents]# chown root:guest /home/guest/Documents/readfile
[root@eademidova Documents]# chmod u+s /home/guest/Documents/readfile
[root@eademidova Documents]# exit
logout
[guest@eademidova Documents]$ ./readfile readfile.c
#include <fcntl.h>
[guest@eademidova Documents]$ ./readfile /etc/sh
shadow shadow- shells
[guest@eademidova Documents]$ ./readfile /etc/shadow
root:$6$c/APB9DR[guest@eademidova Documents]$
```

Рис. 10: Установка SetUID-бита на исполняемый файл readfile и проверка прав

Изменение и проверка прав доступа

```
guest2@eademidova:~$ ls -l / | grep tmp
drwxrwxrwt, 17 root root 4096 Jul  6 14:34 tmp
[guest2@eademidova Documents]$ echo "test" > /tmp/file01.txt
[guest2@eademidova Documents]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Jul  6 14:43 /tmp/file01.txt
[guest2@eademidova Documents]$ chmod o+r /tmp/file01.txt
[guest2@eademidova Documents]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Jul  6 14:43 /tmp/file01.txt
[guest2@eademidova Documents]$ su - guest2
Password:
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@eademidova ~]$ su -
Password:
[root@eademidova ~]# chmod -t /tmp/
[root@eademidova ~]# exit
logout
[guest2@eademidova ~]$ ls -l / | grep tmp
drwxrwxrwx, 18 root root 4096 Jul  6 14:50 tmp
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@eademidova ~]$ cat /tmp/file01.txt
test
[guest2@eademidova ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@eademidova ~]$ ls -l /tmp/
```

Рис. 11: Подключение образа диска дополнений

Заключение

В результате выполнения работы были приобретены практические навыки работы в консоли с расширенными атрибутами файлов.

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