

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ким М. А.

7 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ким Михаил Алексеевич
- студент уч. группы НФИбд-01-20
- Российский университет дружбы народов
- 1032201664@pfur.ru
- <https://github.com/exmanka>



Вводная часть

Актуальность

- Необходимость навыков работы с различными ОС, git, Markdown.

Объект и предмет исследования

- Операционная система Rocky Linux
- Атрибуты файлов и директорий в Linux
- Язык разметки Markdown

Цели и задачи

- 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.

Процесс выполнения работы

Создание программ и изучение SetUID- и SeetGUI-битов. 1

```
guest@makim:~ nano simpleid.c


```

0999 name:9.8.1 stepfield.c notified
#include <sys/types.h>
#include <curlist.h>
#include <ctdlist.h>

int main ()
{
 uid_t uid = geteuid ();
 gid_t gid = getegid ();
 printf ("simpleid: %dmn(%u, %u, %u)\n",
 uid, gid);
 return 0;
}

```


```

File Name to Write: simpleid.c

	M-DOS Format	Append	Backup File
simpleid.c	simpleid.c	simpleid.c	simpleid.c.bak

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

Создание программ и изучение SetUID- и SeetGUI-битов. 2

```
[root@makim ~]# chown root:guest /home/guest/simpleid2
[root@makim ~]# chmod u+s /home/guest/simpleid2
```

```
[root@makim ~]# ll simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 simpleid2
[guest@makim ~]$ ./simpleid2
euid=1001, egid=1001
pid=1393, ppid=1, gtpid=1001
[guest@makim ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0,c1023
```

```
[root@makim ~]# ll simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 simpleid2
[guest@makim ~]$ su -
Password:
[guest@makim ~]$ cd /home/guest/simpleid2
[guest@makim ~]$ ./simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 /home/guest/simpleid2
[guest@makim ~]$ ./simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 /home/guest/simpleid2
[guest@makim ~]$ ./simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 /home/guest/simpleid2
[guest@makim ~]$ exit
[guest@makim ~]$ ll simpleid2
-rwxr-x-- 1 root guest 20994 Oct 7 16:54 simpleid2
[guest@makim ~]$ ./simpleid2
euid=1001, egid=1001
real_euid=1001, real_egid=1001
[guest@makim ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0,c1023
```

Создание программ и изучение SetUID- и SetGUI-битов. Задание

```
[guest@makim ~]$ su -  
Password:  
[root@makim ~]# chmod 700 /home/guest/readfile.c  
[root@makim ~]# chmod 700 /home/guest/readfile.c  
[root@makim ~]# ll /home/guest/readfile.c  
-rwx----- 1 root guest 418 Oct 7 17:20 /home/guest/readfile.c  
[root@makim ~]# exit  
logout  
[guest@makim ~]$ cat readfile.c  
cat: readfile.c: Permission denied
```

```
[guest@zakim ~]$ ll
total 100
drwxr-xr-x 2 guest guest 6 Sep 16 18:20 Desktop
drwxr-xr-x 2 guest guest 19 Sep 30 18:06 dirl
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Documents
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Downloads
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Music
drwxr-xr-x 2 guest guest 100 Sep 16 21:21 Pictures
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Public
drwxr-xr-x 1 guest guest 260888 Oct 7 17:27 readfile
-rwxr--r-- 1 root guest 418 Oct 7 17:20 readfile.c
-rwxr--r-- 1 guest guest 1209 Sep 16 21:14 script_lab02.sh
-rwxr--r-- 1 guest guest 250960 Oct 7 16:52 simpleid
-rwxr--r-- 1 guest guest 260664 Oct 7 16:54 simpleid0
-rwxr--r-- 1 guest guest 312 Oct 7 16:54 simpleid2.c
-rwxr--r-- 1 guest guest 181 Oct 7 16:52 simpleid.c
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Templates
drwxr-xr-x 2 guest guest 6 Sep 16 18:29 Videos
[guest@zakim ~]$ su -
Password:
[root@zakim ~]# chmod root:guest /home/guest/readfile
[root@zakim ~]# chmod u+s /home/guest/readfile
[root@zakim ~]# ll /home/guest/readfile
-rwxr--r-- 1 root guest 260888 Oct 7 17:27 /home/guest/readfile
[root@zakim ~]# exit
logout
```

```
[question]# ./readfile script_label.sh
#!/bin/bash

echo "Starting maxim's script for checking file usability!"

read -p "Enter file! chmod current numeric code: " fileinum
echo "*****"
echo "#1. Trying to create file..." 
(umaxk 777 touch /home/guest/drifile/temp1)
echo "*****"
echo "#2. Trying to remove file..." 
rm /home/guest/drifile/temp1
echo "*****"
echo "#3. Trying to write to file..." 
echo "test" > /home/guest/drifile/file1
echo "*****"
echo "#4. Trying to read file..." 
cat /home/guest/drifile/file1
echo "*****"
echo "#5. Trying to change directory..." 
cd /home/guest/drifile
echo "*****"
echo "#6. Trying to view files in directory..." 
ls -l /home/guest/drifile
echo "*****"
echo "#7. Trying to rename file..." 
(umaxk 777 mv /home/guest/drifile/file1 /home/guest/drifile/temp2)
(umaxk 777 mv /home/guest/drifile/temp2 /home/guest/drifile/file1)
echo "*****"
echo "#8. Trying to change attributes..." 
chmod 0777 /home/guest/drifile/file1
echo "*****"
[question]# ./readfile readable.c
#include <cfntl.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

int main (int argc, char* argv[])
{
    unsigned char buffer[10];
    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;
}

[question]# ./readfile c
cat: readable.c: Permission denied
```

Создание программ и изучение SetUID- и SeetGUI-битов. 4

```
[guest@makin ~]$ ./readfile /etc/shadow
root:$6$1ERU16610Ltu4Y$eNf1Y3nLGSN58EfHy2P3yBL8BVVoyHpGEY1LfB9kp0kHo64wa/1Bw26J2..66HqBNHO2xqH.o7nc0hw.8eKSeQ1::0:
99999:7:::
bin:*:19469:0:99999:7:::
daemon:*:19469:0:99999:7:::
adm:*:19469:0:99999:7:::
lp:*:19469:0:99999:7:::
sync:*:19469:0:99999:7:::
shutdown:*:19469:0:99999:7:::
halt:*:19469:0:99999:7:::
mail:*:19469:0:99999:7:::
operator:*:19469:0:99999:7:::
games:*:19469:0:99999:7:::
ftp:*:19469:0:99999:7:::
nobody:*:19469:0:99999:7:::
systemd-coredump!!!:19609:::::
dbus!!!:19609:::::
polkittd!!!:19609:::::
avahi!!!:19609:::::
rtkit!!!:19609:::::
sssd!!!:19609:::::
pipewire!!!:19609:::::
libstoragemgr!!!:19609:::::
systemd-nommu!!!:19609:::::
tss!!!:19609:::::
geoclue!!!:19609:::::
cockpit-ws!!!:19609:::::
cockpit-wsinstance!!!:19609:::::
flatpak!!!:19609:::::
colorl!!!:19609:::::
clevis!!!:19609:::::
setroubleshoot!!!:19609:::::
gdm!!!:19609:::::
pesign!!!:19609:::::
gnome-initial-setup!!!:19609:::::
sshd!!!:19609:::::
chrony!!!:19609:::::
dnsmasq!!!:19609:::::
tcpdump!!!:19609:::::
makim:$6$F5tUHzcvOH7LwMIUSeZcJj7iC5nD.WAAwEg0YJ6JItYP4uncCozd1bRdmzMA3bG826twcfVYFpSRcIM.E./lKIgK/:19609:0:99999:7:::
:
vboxadd!!!:19609:::::
guest:$6$95c15eydcrxwlnF$M1bG98XssJy239sjoRh9p/1YyDN.FW9500vYV9tcb8Vnp3ksz0DyFkppw7qtNdxlj0Kb6WCH5wuSEHPVqlpsh.:19610:0:99999:7:::
guest2:$6$ta5rDVY32KWF1jP$cQtbx1YRlb1959z5KAKJSAxQI8yE3hqBHUyLl+iuCu1TtcefsyQdt.gMd1RubJVVXZAFN05swJba.MFU4/tD50:1
9623:0:99999:7:::
[guest@makin ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Исследование Sticky-бита. 1

```
[iquest@makim ~] ll | grep tmp  
drwxrwxrwt. 14 root root 4096 Oct 7 17:28 tmp  
[iquest@makim ~] ls echo "test" > /tmp/file01.txt  
[iquest@makim ~] ll /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 Oct 7 17:32 /tmp/file01.txt  
[iquest@makim ~] chmod u+rw /tmp/file01.txt  
[iquest@makim ~] ll /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 Oct 7 17:32 /tmp/file01.txt
```

```
[guest2@makim guest]$ cat /tmp/file01.txt
test
[guest2@makim guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@makim guest]$ cat /tmp/file01.txt
test
[guest2@makim guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@makim guest]$ cat /tmp/file01.txt
test
[guest2@makim guest]$
```

```
[guest2@makim guest]$ rm /tmp/file01.txt  
rm: remove write-protected regular file '/tmp/file01.txt'? y  
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Исследование Sticky-бита. 2

```
[guest2@makim guest]$ su -
Password:
[root@makim ~]# chmod +t /tmp
[root@makim ~]# exit
logout
[guest2@makim guest]$ █
```

Результаты

Результаты

- Выполнены все необходимые задания.

Вывод

Изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.