Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Дорофеева Алёна Тимофеевна

7 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Дорофеева Алёна Тимофеевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201392@pfur.ru
- https://github.com/DorofeevaAT

Вводная часть

Актуальность

- Необходимость понимания возможножностей, предоставляемых различными правами и атрибутами доступа для пользователей.

Объект и предмет исследования

- Применение SetUID-, SetGID- и Sticky-битов.

Цели и задачи

- Изучить на практике действие SetUID-, SetGID- и Sticky-битов.

Материалы и методы

- Командная строка ОС Linux

Процесс выполнения работы

Создание программы simpleid.c

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

```
[guest@aldoro ~]$ touch simpleid
[guest@aldoro ~]$ nano simpleid
[guest@aldoro ~]$ cat simpleid
#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;
}
[guest@aldoro ~]$ gcc simpleid.c -o simpleid
cc1: fatal error: simpleid.c: No such file or directory
compilation terminated.
[guest@aldoro ~]$ mv simpleid simpleid.c
[guest@aldoro ~]$ gcc simpleid.c -o simpleid
[guest@aldoro ~]$ gcc -c simpleid.c
[guest@aldoro ~]$ ls
```

Выполнение программы simpleid.c

```
[guest@aldoro ~]$ ./simpleid
uid=1001, gid=1001
[guest@aldoro ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023
[guest@aldoro ~]$
```

Программа simpleid2.c

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

```
[guest@aldoro ~]$ nano simpleid2.c
[guest@aldoro ~]$ cat simpleid2.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;
}
[guest@aldoro ~]$ ls
Desktop  Documents  Music     Public    simpleid2.c  simpleid.o  Videos
dir1     Downloads  Pictures  simpleid  simpleid.c   Templates
[guest@aldoro ~]$ gcc simpleid2.c -o simpleid2
[guest@aldoro ~]$ ./simpleid2
```

Изменение прав доступа

```
[guest@aldoro ~]$ su aldoro
Password:
[aldoro@aldoro guest]$ sudo -i
[sudo] password for aldoro:
[root@aldoro ~]# chown root:guest /home/guest/simpleid2
[root@aldoro ~]# chmod u+s /home/guest/simpleid2
[root@aldoro ~]#
```

```
[aldoro@aldoro guest]$ su guest
Password:
[guest@aldoro ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Oct 12 05:09 simpleid2
[guest@aldoro ~]$
```

Выполнение программы simpleid2.c

```
[guest@aldoro ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@aldoro ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023
[guest@aldoro ~]$
```

Назначение SetGID-бита

```
[guest@aldoro ~]$ su aldoro
Password:
[aldoro@aldoro guest]$ sudo -i
[root@aldoro ~]# chown root:root /home/guest/simpleid2
[root@aldoro ~]# chmod g+s /home/guest/simpleid2
[root@aldoro ~]#
```

Запуск программы

```
[aldoro@aldoro guest]$ su guest
Password:
[guest@aldoro ~]$ ls -l simpleid2
-rwxr-sr-x. 1 root root 26064 Oct 12 05:09 simpleid2
[guest@aldoro ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@aldoro ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023
[guest@aldoro ~]$
```

Программа readfile.c

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

```
[guest@aldoro ~]$ touch readfile.c
[guest@aldoro ~]$ nano readfile.c
[guest@aldoro ~]$ 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;
```

Смена прав доступа

```
[guest@aldoro ~]$ su aldoro
Password:
[aldoro@aldoro guest]$ sudo -i
[sudo] password for aldoro:
[root@aldoro ~]# chown root:guest /home/guest/readfile.c
[root@aldoro ~]# chmod 733 /home/guest/readfile.c
[root@aldoro ~]#
```

```
[aldoro@aldoro guest]$ su guest
Password:
[guest@aldoro ~]$ ls -l readfile.c
-rwx-wx-wx. 1 root guest 402 Oct 12 05:19 readfile.c
[guest@aldoro ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@aldoro ~]$
```

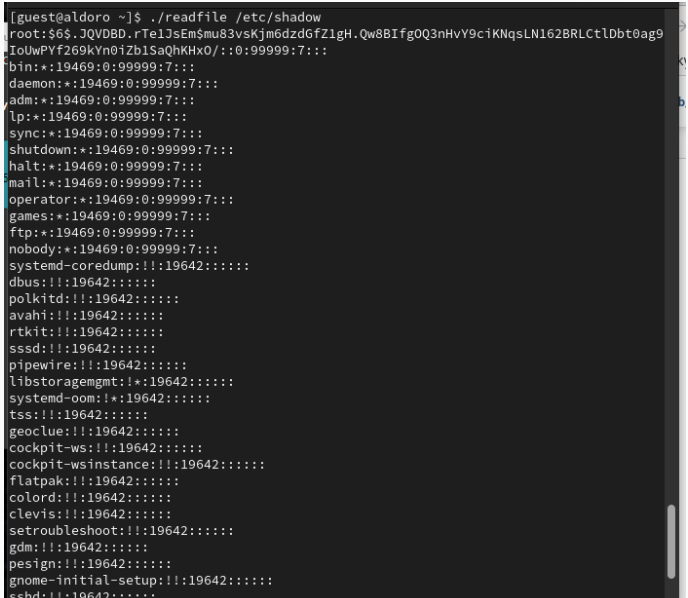
Добавление SetUID-бита

```
[aldoro@aldoro guest]$ sudo -i
[root@aldoro ~]# chown root:guest /home/guest/readfile
[root@aldoro ~]# chmod u+s /home/guest/readfile
[root@aldoro ~]#
```

Попытка чтения файла readfile.c

```
[guest@aldoro ~]$ ./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;
}
[guest@aldoro ~]$
```

Попытка чтения файла /etc/shadow



Проверка наличия STICKY-бита на директории tmp и создание тестового файла

```
[aldoro@aldoro guest]$ sudo -i
[root@aldoro ~]# ls -l / | grep tmp
drwxrwxrwt.  20 root root 4096 Oct 12 05:27 tmp
[root@aldoro ~]#
```

```
[guest@aldoro ~]$ echo "test" > /tmp/file01.txt
[guest@aldoro ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct 12 05:30 /tmp/file01.txt
[guest@aldoro ~]$ chmod o+rw /tmp/file01.txt
[guest@aldoro ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct 12 05:30 /tmp/file01.txt
[guest@aldoro ~]$
```

Попытка дозаписи и записи в файл и его удалениие

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

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

Удаление STICKY-бита

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

Попытка дозаписи и записи в файл и его удаление

```
[guest2@aldoro guest]$ ls -l / | grep tmp
drwxrwxrwx.  18 root root 4096 Oct 12 05:35 tmp
[guest2@aldoro guest]$ cat /tmp/file01.txt
test
[guest2@aldoro guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aldoro guest]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@aldoro guest]$ cat /tmp/file01.txt
test
[guest2@aldoro guest]$
```

```
[guest2@aldoro guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@aldoro guest]$
```

Результаты работы

Результаты работы

- Изучила на практике действие SetUID-, SetGID- и Sticky-битов.

Вывод

Вывод

Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.

Получила практические навыки работы в консоли с дополнительными атрибутами.

Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.