

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ильин А.В.

7 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Ильин Андрей Владимирович
- НФИбд-01-20
- 1032201656
- Российский Университет Дружбы Народов
- 1032201656@pfur.ru
- <https://github.com/av-ilin>



Вводная часть

- Приобрести необходимые в современном научном сообществе навыки администрирования систем и информационной безопасности.

- 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. Создать программу способную выводить `gid`, `uid` и провести исследование SetUID-битов.
2. Исследовать Sticky-бит.

- Rocky Linux
- Git
- VirtualBox

Выполнение работы

simpleid.c и simpleid2.c

```
[guest@aviljin lab05]$ gcc simpleid.c -o simpleid
[guest@aviljin lab05]$ ./simpleid
uid=1001, gid=1001
[guest@aviljin lab05]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@aviljin lab05]$ gcc simpleid2.c -o simpleid2
[guest@aviljin lab05]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 1: Запуск simpleid.c и simpleid2.c

simpleid2.c с измененным владельцем и атрибутами

```
[guest@aviljin lab05]$ su
Password:
[root@aviljin lab05]# chown root:guest simpleid2
[root@aviljin lab05]# chmod u+s simpleid2
[root@aviljin lab05]# exit
exit
[guest@aviljin lab05]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26000 Oct  7 19:08 simpleid2
[guest@aviljin lab05]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@aviljin lab05]$ su
Password:
[root@aviljin lab05]# chmod u-s simpleid2
[root@aviljin lab05]# chmod g+s simpleid2
[root@aviljin lab05]# exit
exit
[guest@aviljin lab05]$ ls -l simpleid2
-rwxr-sr-x. 1 root guest 26000 Oct  7 19:08 simpleid2
[guest@aviljin lab05]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 2: Запуск simpleid2.c с измененным владельцем и атрибутами

Подготовка к запуску readfile

```
[guest@aviljin lab05]$ su
Password:
[root@aviljin lab05]# chown root:guest readfile.c
[root@aviljin lab05]# chmod 700 readfile.c
[root@aviljin lab05]# ls -l readfile.c
-rwx-----. 1 root guest 455 Oct  7 19:07 readfile.c
[root@aviljin lab05]# exit
exit
[guest@aviljin lab05]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@aviljin lab05]$ su
Password:
[root@aviljin lab05]# chown root:guest readfile
[root@aviljin lab05]# chmod u+s readfile
[root@aviljin lab05]# ls -l readfile
-rwsr-xr-x. 1 root guest 25952 Oct  7 19:40 readfile
```

Рис. 3: Подготовка к запуску readfile

Запуск readfile

```
hguest@aviljin lab05]$ ./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;
}hguest@aviljin lab05]$
```

Рис. 4: Запуск readfile (readfile.c)

```
hguest@aviljin lab05]$ ./readfile /etc/shadow
root:$6$ty/.S./YlK1GzplF$AhzG3919.GSkS1Q9h13Gand8dUhd8vzWBN7S96J4uud0b8t4F4Kf1cB918B8GPD43sb.PtuHmJ6
/46ev$8x.c8:0:99999:7:::
bin:0:19469:0:99999:7:::
daemon:0:19469:0:99999:7:::
adm:0:19469:0:99999:7:::
lp:0:19469:0:99999:7:::
sync:0:19469:0:99999:7:::
shutdown:0:19469:0:99999:7:::
halt:0:19469:0:99999:7:::
mail:0:19469:0:99999:7:::
operator:0:19469:0:99999:7:::
games:0:19469:0:99999:7:::
ftp:0:19469:0:99999:7:::
nobody:0:19469:0:99999:7:::
system-coredump:!!:19688:!!!!:
dbus:!!:19688:!!!!:
tss:!!:19688:!!!!:
sssd:!!:19688:!!!!:
sshd:!!:19688:!!!!:
chromy:!!:19688:!!!!:
system-oom:!:19688:!!!!:
aviljin:$6$4sCrUQ2Ptw4pEda$8.jcQaFthE6.jRBkymWohs.vQ11MqP.5e0aEacMbfGIRp.8aEZAr91Rb8BShmyKV1jQK3rIP2
sE11.7rifuWkx0:19688:0:99999:7:::
guest:$6$C1sUY0y8GSY1tawp$FQs3U6rwJabTh0hqdGLyX1W9fgt2T.hMpX0cCnHBp11w11FMBXq0C8Hq4SK4AkSmkTsUSFN3fc
K/zulh5CKDov:19616:0:99999:7:::
guest2:$6$29g46Z0N3X4MxqvUSN2ef1hsyBmJ3bC4z5oGUqwm5o0yH2J2.ppSabb8G1h8N2rLkFmJv1jtaH39/XfKtwImKcnQs
SHKFn0pJm0B:19623:0:99999:7:::
```

Рис. 5: Запуск readfile (/etc/shadow)

Подготовка к исследованию Sticky-бита

```
lguest@aviljin ~]$ ls -l / | grep tmp
drwxrwxrwt.  5 root root 4096 Oct  7 19:59 tmp
lguest@aviljin ~]$ echo "test" > /tmp/file01.txt
lguest@aviljin ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  7 20:06 /tmp/file01.txt
lguest@aviljin ~]$ chmod o+rw /tmp/file01.txt
lguest@aviljin ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  7 20:06 /tmp/file01.txt
lguest@aviljin ~]$ _
```

Рис. 6: Атрибут Sticky

Исследование Sticky-бита

```
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
fguest2@aviljin ~]$ _
```

Рис. 7: Исследование Sticky (1)

```
fguest2@aviljin ~]$ su -
Password:
Last login: Sat Oct 7 20:13:58 MSK 2023 on tty4
[root@aviljin ~]# chmod -t /tmp
[root@aviljin ~]# exit
logout
fguest2@aviljin ~]$ ls -l / | grep tmp
drwxrwxrwt. 6 root root 4096 Oct 7 20:17 tmp
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
fguest2@aviljin ~]$ cat /tmp/file01.txt
test
fguest2@aviljin ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
fguest2@aviljin ~]$ su -
Password:
Last login: Sat Oct 7 20:17:09 MSK 2023 on tty4
[root@aviljin ~]# chmod +t /tmp
[root@aviljin ~]# exit
logout
fguest2@aviljin ~]$ ls -l / | grep tmp
drwxrwxrwt. 6 root root 4096 Oct 7 20:17 tmp
```

Рис. 8: Исследование Sticky (2)

Результаты

- Изучены идентификаторы SetUID-биты и Sticky-биты. Опробовали их действие на практике. Изучили влияние бита Sticky. Повысили свои навыки использования интерфейса командой строки (CLI).

Спасибо за внимание!