

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ласурия Данил

8 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

Цель лабораторной работы

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.

Выполнение лабораторной работы

Программа simpleid

```
[root@localhost lasuriyadr]# whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.info.gz
[root@localhost lasuriyadr]# touch simpleid.c
[root@localhost lasuriyadr]# nano simpleid.c
[root@localhost lasuriyadr]# gcc simpleid.c -o simpleid
[root@localhost lasuriyadr]# ./simpleid
uid=0, gid=0
[root@localhost lasuriyadr]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 1: результат программы simpleid

Программа simpleid2

```
File Edit View Search Terminal Help
[guest@localhost ~]$ nano simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$ su
Password:
su: Authentication failure
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]#
[root@localhost guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 18256 Oct  8 18:48 simpleid2
[root@localhost guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[root@localhost guest]# nano readfile.c
[root@localhost guest]# gcc readfile.c -o readfile
[root@localhost guest]# chown root:root readfile
```

Figure 2: результат программы simpleid2

Программа readfile

```
root@localhost:~# nano readfile.c
[root@localhost guest]# gcc readfile.c -o readfile
[root@localhost guest]# chown root:root readfile
bash: chown: command not found...
[root@localhost guest]# chown root:root readfile
[root@localhost guest]# chmod -r readfile.c
[root@localhost guest]# chmod u+s readfile
[root@localhost guest]# exit
exit
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@localhost ~]$ ./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;
}
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
if [ $(cat /etc/passwd | grep guest | wc -l) -eq 0 ]; then echo "No guest user found" && exit 1; fi
[guest@localhost ~]$ cd /tmp
[guest@localhost tmp]$ echo "tst" >> file0.txt
[guest@localhost tmp]$ chmod o+rw file0.txt
[guest@localhost tmp]$ ls -l file0.txt
-rw-rw-rw-. 1 guest guest 4 Oct  8 18:54 file0.txt
[guest@localhost tmp]$ su guest2
Password:
[guest2@localhost tmp]$ cat /tmp/file0.txt
cat: /tmp/file0.txt: No such file or directory
[guest2@localhost tmp]$ cat file0.txt
cat: file0.txt: No such file or directory
[guest2@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-w0qxii
systemd-private-d1d3dd623d3b467692c032d10c883cfe-colord.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fprintd.service-e0qe0b
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-n0A19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VnmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YG5G17
tracker-extract-files-1000
[guest2@localhost tmp]$ su guest
Password:
[guest@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-w0qxii
systemd-private-d1d3dd623d3b467692c032d10c883cfe-colord.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fprintd.service-YvwlZ9
systemd-private-d1d3dd623d3b467692c032d10c883cfe-fwupd.service-gLWgIP
systemd-private-d1d3dd623d3b467692c032d10c883cfe-geoclue.service-n0A19T
systemd-private-d1d3dd623d3b467692c032d10c883cfe-ModemManager.service-K6VnmY
systemd-private-d1d3dd623d3b467692c032d10c883cfe-rtkit-daemon.service-YG5G17
tracker-extract-files-1000
[guest@localhost tmp]$ su guest 2
Password:
bash: 2: No such file or directory
[guest@localhost tmp]$ su guest2
Password:
[guest2@localhost tmp]$ ls
file0.txt
systemd-private-d1d3dd623d3b467692c032d10c883cfe-chrond.service-w0qxii
systemd-private-d1d3dd623d3b467692c032d10c883cfe-colord.service-YvwlZ9
```

Figure 4: исследование Sticky-бита

Выводы

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.