

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Балтаева Галина НПИбд-01-19

5 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

```
[guest@gnbaltaeva ~]$  
[guest@gnbaltaeva ~]$  
[guest@gnbaltaeva ~]$ mkdir lab5  
[guest@gnbaltaeva ~]$ cd lab5/  
[guest@gnbaltaeva lab5]$ touch simpleid.c  
[guest@gnbaltaeva lab5]$ touch simpleid2.c  
[guest@gnbaltaeva lab5]$ touch redfile.c  
[guest@gnbaltaeva lab5]$  
[guest@gnbaltaeva lab5]$ gedit simpleid.c  
[guest@gnbaltaeva lab5]$ gcc simpleid.c  
[guest@gnbaltaeva lab5]$ gcc simpleid.c -o simpleid  
[guest@gnbaltaeva lab5]$ ./simpleid  
uid=1001, gid=1001  
[guest@gnbaltaeva lab5]$ id  
uid=1001(guest) gid=1001(guest) rpnны=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@gnbaltaeva lab5]$
```

Figure 1: результат программы simpleid

Программа simpleid2

```
[guest@gnbaltaeva lab5]$ ./simpleid2
bash: ./simpleid2: Нет такого файла или каталога
[guest@gnbaltaeva lab5]$ ./simpleid2.c
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@gnbaltaeva lab5]$ mv simpleid2.c simpleid2
[guest@gnbaltaeva lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@gnbaltaeva lab5]$ su
Пароль:
[root@gnbaltaeva lab5]# chown root:guest simpleid2
[root@gnbaltaeva lab5]# chmod u+s simpleid2
[root@gnbaltaeva lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@gnbaltaeva lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@gnbaltaeva lab5]# chmod g+s simpleid2
[root@gnbaltaeva lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@gnbaltaeva lab5]#
```

Figure 2: результат программы simpleid2

Программа readfile

```
[guest@gnbaltaeva lab5]#  
[guest@gnbaltaeva lab5]$ gedit redfile.c  
[guest@gnbaltaeva lab5]$ gcc redfile.c  
redfile.c: В функции «main»:  
redfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию вклю  
чена]  
    while (bytes_read == (buffer));  
                    ^  
[guest@gnbaltaeva lab5]$ gcc redfile.c -o readfie  
redfile.c: В функции «main»:  
redfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию вклю  
чена]  
    while (bytes_read == (buffer));  
                    ^  
[guest@gnbaltaeva lab5]$ su  
Пароль:  
[root@gnbaltaeva lab5]# chown root:root readfie  
[root@gnbaltaeva lab5]# chmod -r redfile.c  
[root@gnbaltaeva lab5]# chmod u+s readfie  
[root@gnbaltaeva lab5]# exit  
exit  
[guest@gnbaltaeva lab5]$ cat redfile.c  
cat: redfile.c: Отказано в доступе  
[guest@gnbaltaeva lab5]$ ./readfie redfile.c  
#include <stdio.h>[guest@gnbaltaeva lab5]$ ./readfie /etc/shadow  
root:$6$FR5m5KGe'[guest@gnbaltaeva lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита

```
[guest@gnbaltaeva lab5]$  
[guest@gnbaltaeva lab5]$  
[guest@gnbaltaeva lab5]$ echo "test" >> /tmp/file01.txt  
[guest@gnbaltaeva lab5]$ cd /tmp  
[guest@gnbaltaeva tmp]$ chmod o+rx file01.txt  
[guest@gnbaltaeva tmp]$ ls -l file01.txt  
-rw-rw-r-x. 1 guest guest 5 окт  5 10:40 file01.txt  
[guest@gnbaltaeva tmp]$ su guest2  
Пароль:  
[guest2@gnbaltaeva tmp]$ cat file01.txt  
test  
[guest2@gnbaltaeva tmp]$ echo "test" >> file01.txt  
[guest2@gnbaltaeva tmp]$ echo "test" > file01.txt  
[guest2@gnbaltaeva tmp]$ rm file01.txt  
rm: невозможно удалить «file01.txt»: Операция не позволена  
[guest2@gnbaltaeva tmp]$ su  
Пароль:  
[root@gnbaltaeva tmp]# chmod -t /tmp/  
[root@gnbaltaeva tmp]# exit  
exit  
[guest2@gnbaltaeva tmp]$ rm file01.txt  
[guest2@gnbaltaeva tmp]$ su  
Пароль:  
[root@gnbaltaeva tmp]# chmod +t /tmp/  
[root@gnbaltaeva tmp]#
```

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.