

Презентация к лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

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

Выполнение лабораторной работы

Создание программы

Создал программу simpleid.c

```
[guest@localhost ~]$ ls
dir1  Видео      Загрузки      Музыка      'Рабочий стол'
file1 Документы  Изображения  Общедоступные  Шаблоны
[guest@localhost ~]$ touch simpleid.c
[guest@localhost ~]$ ls
dir1  simpleid.c  Документы  Изображения  Общедоступные  Шаблоны
file1 Видео      Загрузки      Музыка      'Рабочий стол'
```

Записал код программы в simpleid.c

```
#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;
}
```

Скомпилировал и выполнил программу simpleid.c

```
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ls
file1  simpleid  Видео      Загрузки  Музыка     'Рабочий стол'
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
```


Изменил код программы в simpleid.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;
}
```

Получившуюся программу назовите simpleid2.c.

Скомпилируйте и запустите simpleid2.c:

```
gcc simpleid2.c -o simpleid2
```

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

От имени суперпользователя поменял права на файл simpleid2.c, поменял владельца файла и выполнил программу

```
[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 17656 окт  5 18:46 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) rpyнны=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost guest]# touch readfile.c
[root@localhost guest]# ls
file1 simpleid2 Видео Изображения 'Рабочий стол'
readfile.c simpleid.c Документы Музыка Шаблоны
Загрузки Общедоступные
```

- Результаты выполнения отличаются.

Создал файл readfile.c

```
[root@localhost guest]# touch readfile.c
[root@localhost guest]# ls
dir1          simpleid      Видео         Изображения   'Рабочий стол'
file1         simpleid2     Документы     Музыка         Шаблоны
readfile.c    simpleid.c    Загрузки     Общедоступные
```

Записал код программы в 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@localhost ~]$ gcc readfile.c -o readfile
```

Сменил права и владельца readfile.c, попробовал от имени пользователя guest прочитать файл, получил отказ

```
[root@localhost guest]# chown root:ilya readfile.c
[root@localhost guest]# ls -l readfile.c
-rw-r--r--. 1 root ilya 402 окт  5 19:28 readfile.c
[root@localhost guest]# chmod 700 readfile.c
[root@localhost guest]# ls -l readfile.c
-rwx-----. 1 root ilya 402 окт  5 19:28 readfile.c
[root@localhost guest]# su guest
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
```

С помощью программы readfile прочитал файл /etc/shadow

```
[root@localhost guest]# ./readfile /etc/shadow
root:$6$ErPFI12NochdKwF1$1N3ddm1Jmh3R1zuYDMG9BgN3r8Mon/y3Y1tDkZ0cyvPwt1JbLYm4WYFsXTibQtFQgiLjnA04S.hff06yp0vVQ.::0:99999:7:::
bin:!:19760:0:99999:7:::
daemon:!:19760:0:99999:7:::
adm:!:19760:0:99999:7:::
lp:!:19760:0:99999:7:::
sync:!:19760:0:99999:7:::
shutdown:!:19760:0:99999:7:::
halt:!:19760:0:99999:7:::
mail:!:19760:0:99999:7:::
operator:!:19760:0:99999:7:::
games:!:19760:0:99999:7:::
ftp:!:19760:0:99999:7:::
nobody:!:19760:0:99999:7:::
tss:!:19973:!:!:!:
systemd-coredump:!:19973:!:!:!:
dbus:!:19973:!:!:!:
polkitd:!:19973:!:!:!:
avahi:!:19973:!:!:!:
geoclue:!:19973:!:!:!:
rtkit:!:19973:!:!:!:
libstoragemgmt:!:19973:!:!:!:
cockpit-wsinstance:!:19973:!:!:!:
colord:!:19973:!:!:!:
sssd:!:19973:!:!:!:
c-levis:!:19973:!:!:!:
setroubleshoot:!:19973:!:!:!:
pipewire:!:19973:!:!:!:
flatpak:!:19973:!:!:!:
gdm:!:19973:!:!:!:
gnome-initial-setup:!:19973:!:!:!:
chrony:!:19973:!:!:!:
sshd:!:19973:!:!:!:
dnsmasq:!:19973:!:!:!:
tcpdump:!:19973:!:!:!:
1lya:$6$Vlh2DW/VduTLtp/g$tsxDLabLmG4f9GUl0861V5jw6F9.298MvE6X8b1l65tqXEJ4F7rRYLR3ow/Y39u1/hSpDZ846udBVoTNJdnq0::0:99999:7:::
guest:$6$rounds=100000$fm6E4jtLNEgmoLX$TSANu3gozjFWIk4due.3LpLXmPKuB.2IkJRYW2FB0j2rRW6v.KVhu.HZNQLzArkvh2r2U3xtWSFEQryzrKKVw0:19980:0:99999:7:::
guest2:$6$rounds=100000$t4sJiQ8jKhr2docMSB0GzE6d3f0EtuFzU5YpEqn5WLcnpmhP8zSZew.TB0CJk7d1fy15ekGlrCKCmr7nr3WvFDX00AFZmqcQrH4r1:19987:0:99999:7:::
```


Исследование Sticky-бита

Проверил установлен ли атрибут Sticky на директории /tmp , создал в ней файл file91.txt

```
[guest@localhost tmp]$ ls -l /| grep tmp
drwxrwxrwt. 19 root root 4096 окт  5 20:06 tmp
[guest@localhost tmp]$ echo "test" > file01.txt
[guest@localhost tmp]$ ls
file01.txt
systemd-private-48c61689454144bab7b1a476779827df-chrond.service-aCJ6zE
systemd-private-48c61689454144bab7b1a476779827df-colord.service-RKN3DX
systemd-private-48c61689454144bab7b1a476779827df-dbus-broker.service-dcYTGF
systemd-private-48c61689454144bab7b1a476779827df-fwupd.service-uV2A1S
systemd-private-48c61689454144bab7b1a476779827df-irqbalance.service-djIAFx
systemd-private-48c61689454144bab7b1a476779827df-kdump.service-oAnE4Y
systemd-private-48c61689454144bab7b1a476779827df-ModemManager.service-o09hBJ
systemd-private-48c61689454144bab7b1a476779827df-power-profiles-daemon.service-4z5gh0
systemd-private-48c61689454144bab7b1a476779827df-rtkit-daemon.service-z8ToXL
systemd-private-48c61689454144bab7b1a476779827df-switcheroo-control.service-9axydX
systemd-private-48c61689454144bab7b1a476779827df-systemd-logind.service-TAhLUp
systemd-private-48c61689454144bab7b1a476779827df-upower.service-mZ0kMT
Tmp-893e9933-5399-4673-b9d2-24bee6eb0acb
tmpaddon
```

Проверил атрибуты у файла file01.txt , поменял атрибуты на чтение и запись для остальных пользователей

```
[guest@localhost tmp]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт  5 20:08 /tmp/file01.txt
[guest@localhost tmp]$ chmod o+rw /tmp/file01.txt
[guest@localhost tmp]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт  5 20:08 /tmp/file01.txt
```

От пользователя guest 2 попробовал прочитать, изменить и удалить file01.txt, получилось только прочитать

```
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ echo "test" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

От имени суперпользователя снял атрибут t у /tmp

```
[root@localhost guest]# chmod -t /tmp
```

От имени guest 2 проверил, что у директории /tmp нет атрибута t. Попробовал сделать команды еще раз, ничего не поменялось.

```
[guest2@localhost guest]$ ls -l / | grep tmp
drwxrwxrwx. 19 root root 4096 окт  5 20:12 tmp
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ echo "test" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
```

Поменял права файла file01.txt на 666

```
[guest@localhost tmp]$ chmod 666 file01.txt  
[guest@localhost tmp]$ ls -l file01.txt
```

Попробовал выполнить команды еще раз, получилось сделать все, кроме удаления

```
[guest2@localhost guest]$ echo "test2" > /tmp/file01.txt
[guest2@localhost guest]$ cat file01.txt
cat: file01.txt: Нет такого файла или каталога
[guest2@localhost guest]$ cat /tmp/file01.txt
test2
[guest2@localhost guest]$ echo "test3" > /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```


Удалил атрибут `t` и выполнил команды, получилось выполнить все, включая удаление

```
[guest2@localhost guest]$ su -  
Пароль:  
[root@localhost ~]# chmod -t /tmp  
[root@localhost ~]# exit  
выход  
[guest2@localhost guest]$ ls -l / | grep tmp  
drwxrwxrwx. 19 root root 4096 окт  5 20:03 tmp  
[guest2@localhost guest]$ cat /tmp/file01.txt  
test3  
[guest2@localhost guest]$ echo "test2" > /tmp/file01.txt  
[guest2@localhost guest]$ cat /tmp/file01.txt  
test2  
[guest2@localhost guest]$ rm /tmp/file01.txt
```

Выводы

Изучил механизм изменения идентификаторов, применяя SetUID и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияния бита Sticky на запись и удаление файлов.