# Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Кекишева А.Д.

25 сентября 2023

Российский университет дружбы народов, Москва, Россия

# Информация

# Докладчик


- Кекишева Анастасия Дмитриевна
- Бизнес-информатика
- Кафедра теории веротности и кибербезопасности
- Российский университет дружбы народов
- 1032201194@pfur.ru
- https://github.com/adkekisheva

# Цель работы

# Цель 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.

# Задание

# Задание

Выполнить последовательность дейсвий, указанных в лабораторной работе, создавая программы и работая с битами (SetUID, SetGID, Sticky-бит), чтобы изучить влияние дополнительных атрибутов.

# Теоретическое введение

Рассмотрим некоторые команды, которые пригодяться нам в данной лабораторной.

- chown [ПАРАМЕТР]... [ВЛАДЕЛЕЦ][:[ГРУППА]] ФАЙЛ... Эта команда позволяет сменить владельца и группу указанного ФАЙЛА на ВЛАДЕЛЬЦА и/или ГРУППУ.
- gcc [ИМЯ_ФАЙЛА].c -o [ИМЯ_ПРОГРАММЫ] Это команда поможет нам конвертировать файлы.

# Выполнение лабораторной работы

# Выполнение лабораторной работы

Изучение механики SetUID

# Шаг 1 - Создание программы simpleid.c

# Шаг 1 - Создание программы simpleid.c

```
<http://bugzilla.redhat.com/bugzilla>.
[adkekisheva@adkekisheva ~]$ su guest1
Password:
[guest1@adkekisheva adkekisheva]$ cd
[guest1@adkekisheva ~]$ ls
Desktop  dir1  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[guest1@adkekisheva ~]$ touch simpleid.c
[guest1@adkekisheva ~]$ cat >> 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;
}
^C
[guest1@adkekisheva ~]$ cat 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;
}
```

# Шаг 2 - Компиляция и запуск программы

# Шаг 2 - Компиляция и запуск программы

```
[guest1@adkekisheva ~]$ gcc simpleid.c -o simpleid
[guest1@adkekisheva ~]$ ./simpleid
uid=1002, gid=1002
[guest1@adkekisheva ~]$ id
uid=1002(guest1) gid=1002(guest1) groups=1002(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 2: Компиляция и запуск программы

# Шаг 3 - Написание программы simpleid2.c

# Шаг 3 - Написание программы simpleid2.c

```
[guest1@adkekisheva ~]$ touch simpleid2.c
[guest1@adkekisheva ~]$ 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;
}
^C
```

Figure 3: Написание программы simpleid2.c

# Шаг 4 - Компиляция и запуск программы simpleid2

# Шаг 4 - Компиляция и запуск программы simpleid2

```
[guest1@adkekisheva ~]$ 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;
}
[guest1@adkekisheva ~]$ gcc simpleid2.c -o simpleid2
[guest1@adkekisheva ~]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
```

# Шаг 5 - Компиляция и запуск программы

# Шаг 5 - Компиляция и запуск программы

```
[root@adkekisheva ~]# chown root:guest1 /home/guest1/simpleid2
[root@adkekisheva ~]# chmod u+s /home/guest1/simpleid2
[root@adkekisheva ~]# ls -l simpleid2
ls: cannot access simpleid2: No such file or directory
[root@adkekisheva ~]# ls
anaconda-ks.cfg  dir1  initial-setup-ks.cfg
[root@adkekisheva ~]# su duest1
su: user duest1 does not exist
[root@adkekisheva ~]# su guest1
[guest1@adkekisheva root]$ cd
[guest1@adkekisheva ~]$ ls
Desktop  Documents  Music     Public    simpleid2    simpleid.c  Videos
dir1     Downloads  Pictures  simpleid  simpleid2.c  Templates
[guest1@adkekisheva ~]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest1 8576 Sep 23 12:17 simpleid2
[guest1@adkekisheva ~]$ ./simpleid2
e_uid=0, e_gid=1002
real_uid=1002, real_gid=1002
[guest1@adkekisheva ~]$ id
uid=1002(guest1) gid=1002(guest1) groups=1002(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 5: Компиляция и запуск программы

# Шаг 6 - Установка SetGID-бита

# Шаг 6 - Установка SetGID-бита

```
[root@adkekisheva ~]# chown root:guest1 /home/guest1/simpleid2
[root@adkekisheva ~]# chmod g+s /home/guest1/simpleid2
[root@adkekisheva ~]# su guest1
[guest1@adkekisheva root]$ cd
[guest1@adkekisheva ~]$ ls -l simpleid2
-rwxrwsr-x. 1 root guest1 8576 Sep 23 12:17 simpleid2
[guest1@adkekisheva ~]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest1@adkekisheva ~]$ id
uid=1002(guest1) gid=1002(guest1) groups=1002(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

**Figure 6:** Установка SetGID-бита

# Шаг 7 - Создание и компиляция программы readfile.c

# Шаг 7 - Создание и компиляция программы readfile.c

```
[guest1@adkekisheva ~]$ 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;
}
[guest1@adkekisheva ~]$ gcc readfile.c -o readfile
[guest1@adkekisheva ~]$ ls -l readfile
-rwxrwxr-x. 1 guest1 guest1 8512 Sep 23 13:13 readfile
```

# Шаг 8 - Настройка прав для файла readfile.c

# Шаг 8 - Настройка прав для файла readfile.c

```
[root@adkekisheva guest1]# chown root:root readfile
[root@adkekisheva guest1]# chmod o-r readfile.c
[root@adkekisheva guest1]# chmod g-rw readfile.c
[root@adkekisheva guest1]# chmod u+s readfile
[root@adkekisheva guest1]# exit
logout
[guest2@adkekisheva ~]$ su guest1
Password:
[guest1@adkekisheva guest2]$ cd
[guest1@adkekisheva ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest1@adkekisheva ~]$ ./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;
}
```

# Шаг 9 - Чтение файла /etc/shadow с помощью программы readfile

# Шаг 9 - Чтение файла /etc/shadow с помощью программы readfile

```
[guest1@adkekisheva ~]$ ./readfile /etc/shadow
root:$6$Y/THRikj/CG6mSx8$g91mJJwqJMCzQ1q/atgY1hjOXdKNMCc2XRdSs5WnxmGL9GVBy1Q2nSD9i9bLXLfQ8SDL4vyi/u7.oAL
ky0::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
systemd-network:!!:19605::::::
dbus:!!:19605::::::
polkitd:!!:19605::::::
libstoragemgmt:!!:19605::::::
colord:!!:19605::::::
rpc:!!:19605:0:99999:7:::
saned:!!:19605::::::
saslauth:!!:19605::::::
abrt:!!:19605::::::
setroubleshoot:!!:19605::::::
rtkit:!!:19605::::::
pulse:!!:19605::::::
radvd:!!:19605::::::
chrony:!!:19605::::::
unbound:!!:19605::::::
qemu:!!:19605::::::
tss:!!:19605::::::
usbmuxd:!!:19605::::::
geoclue:!!:19605::::::
gluster:!!:19605::::::
gdm:!!:19605::::::
rpcuser:!!:19605::::::
```

# Исследование Sticky-бита

## Шаг 1 - Проверка атрибута sticky и создание файла

```
[guest1@adkekisheva ~]$ ls -l / | grep tmp
drwxrwxrwt.  27 root root 4096 Sep 24 15:16 tmp
[guest1@adkekisheva ~]$ echo "test" > /tmp/file01.txt
```

Figure 10: Проверка атрибута sticky и создание файла

## Шаг 2 - Добавление прав остальным пользователям на чтение и запись

# Шаг 2 - Добавление прав остальным пользователям на чтение и запись

```
[guest1@adkekisheva ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest1 guest1 5 Sep 24 15:21 /tmp/file01.txt
[guest1@adkekisheva ~]$ chmod o+rw /tmp/file01.txt
[guest1@adkekisheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest1 guest1 5 Sep 24 15:21 /tmp/file01.txt
[guest1@adkekisheva ~]$ su guest2
Password:
[guest2@adkekisheva guest1]$ cd
[guest2@adkekisheva ~]$ cat /tmp/file01.txt
test
```

Figure 11: Добавление прав остальным пользователям на чтение и запись

## Шаг 3 - Проверка атрибута sticky и создание файла

```
test
[guest2@adkekisheva ~]$ echo "test2" > /tmp/file01.txt
[guest2@adkekisheva ~]$ cat /tmp/file01.txt
test2
[guest2@adkekisheva ~]$ echo "test3" > /tmp/file01.txt
[guest2@adkekisheva ~]$ cat /tmp/file01.txt
test3
[guest2@adkekisheva ~]$ rm /tmp/file01.txt
rm: cannot remove ‘/tmp/file01.txt’: Operation not permitted
[guest2@adkekisheva ~]$ su -
Password:
Last login: Sun Sep 24 13:36:48 MSK 2023 on pts/0
[root@adkekisheva ~]# chmod -t /tmp
[root@adkekisheva ~]# exit
logout
[guest2@adkekisheva ~]$ ls -l / | grep tmp
drwxrwxrwx.  27 root root 4096 Sep 24 15:25 tmp
```

Figure 12: Проверка атрибута sticky и создание файла

# Шаг 4 - Шаги без sticky-бита

# Шаг 4 - Шаги без sticky-бита

```
[guest1@adkekisheva guest2]$ cd
[guest1@adkekisheva ~]$ echo "test" > /tmp/file01.txt
[guest1@adkekisheva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest1 guest1 5 Sep 24 15:54 /tmp/file01.txt
[guest1@adkekisheva ~]$ su guest2
Password:
[guest2@adkekisheva guest1]$ cd
[guest2@adkekisheva ~]$ echo "test2" > /tmo/file01.txt
bash: /tmo/file01.txt: No such file or directory
[guest2@adkekisheva ~]$ echo "test2" > /tmp/file01.txt
[guest2@adkekisheva ~]$ cat /tmp/file01.txt
test2
[guest2@adkekisheva ~]$ echo "test3" > /tmp/file01.txt
[guest2@adkekisheva ~]$ cat /tmp/file01.txt
test3
[guest2@adkekisheva ~]$ rm /tmp/file01.txt
[guest2@adkekisheva ~]$ su -
Password:
Last login: Sun Sep 24 15:24:52 MSK 2023 on pts/0
[root@adkekisheva ~]# ls -l / | grep tmp
drwxrwxrwx.  28 root root 4096 Sep 24 15:56 tmp
[root@adkekisheva ~]# chmod +t /tmp
[root@adkekisheva ~]# ls -l / | grep tmp
drwxrwxrwt.  27 root root 4096 Sep 24 15:56 tmp
[root@adkekisheva ~]# exit
logout
```

# Выводы

# Выводы

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.