Защита лабораторной работы №5 Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Исаханян Эдуард Тигранович

2022 Sep 17th

RUDN University, Moscow, Russian Federation

Защита лабораторной работы №5

Цель

Цель

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.c

```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;
}
```

Figure 1: Программа simpleid.c

Компиляция и выполнение программы simpleid

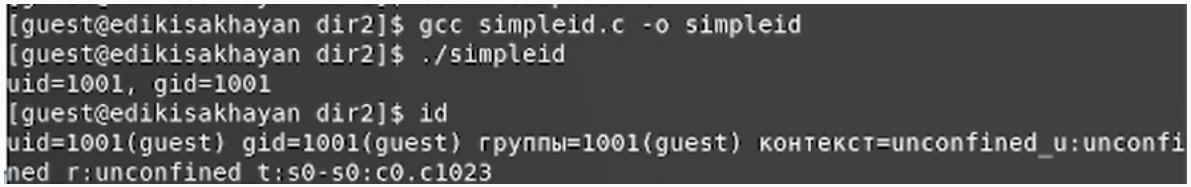

Figure 2: Компиляция и выполнение программы simpleid

Программа simpleid2.c

```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;
}
```

Figure 3: Программа simpleid2.c

Компиляция и выполнение программы simpleid2

```
[guest@edikisakhayan dir2]$ gcc simpleid2.c -o simpleid2
[guest@edikisakhayan dir2]$ ./simpleid2
e_uid=1001, e_gid=1001
real uid=1001, real gid=1001
```

Figure 4: Компиляция и выполнение программы simpleid2

Смена пользователя. Установка SetUID-бита. Выполнение программы simpleid2

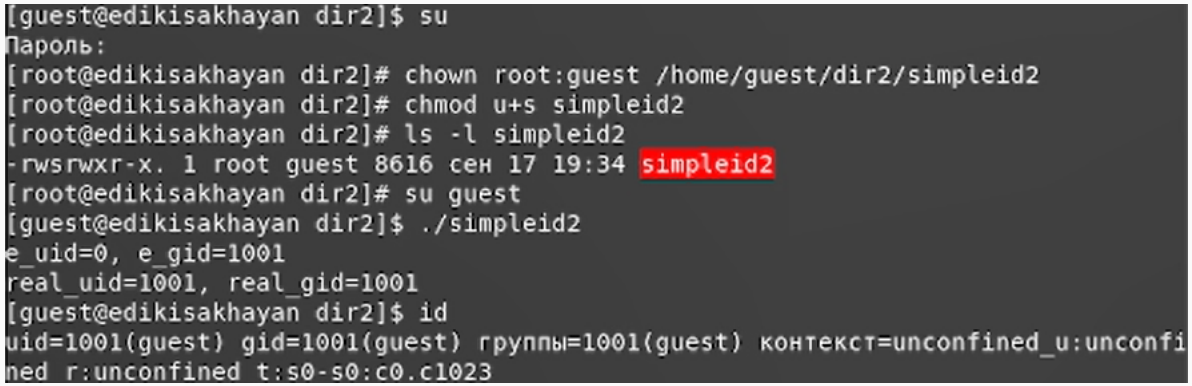

Figure 5: Смена пользователя. Установка SetUID-бита. Выполнение программы simpleid2

Установка SetGID-бита. Выполнение программы simpleid2

Figure 6: Установка SetGID-бита. Выполнение программы simpleid2

Программа readfile.c

```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 7: Программа readfile.c

Работа с программой readfile.c

```
[guest@edikisakhayan dir2]$ gcc readfile.c -o readfile
[guest@edikisakhayan dir2]$ su
Пароль:
[root@edikisakhayan dir2]# chown root:guest readfile.c
[root@edikisakhayan dir2]# chmod 700 readfile.c
[root@edikisakhayan dir2]# su guest
[guest@edikisakhayan dir2]$ cat readfile.c
cat: readfile.c: Отказано в доступе
```

Figure 8: Работа с программой readfile.c

Установка SetUID-бита на программу readfile

```
[root@edikisakhayan dir2]# chown root:guest readfile
[root@edikisakhayan dir2]# chmod u+s readfile
```

Figure 9: Установка SetUID-бита на программу readfile

Программа readfile читает readfile.c

```
[root@edikisakhayan dir2]# ./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 10: Программа readfile читает readfile.c

Программа readfile читает /etc/shadow

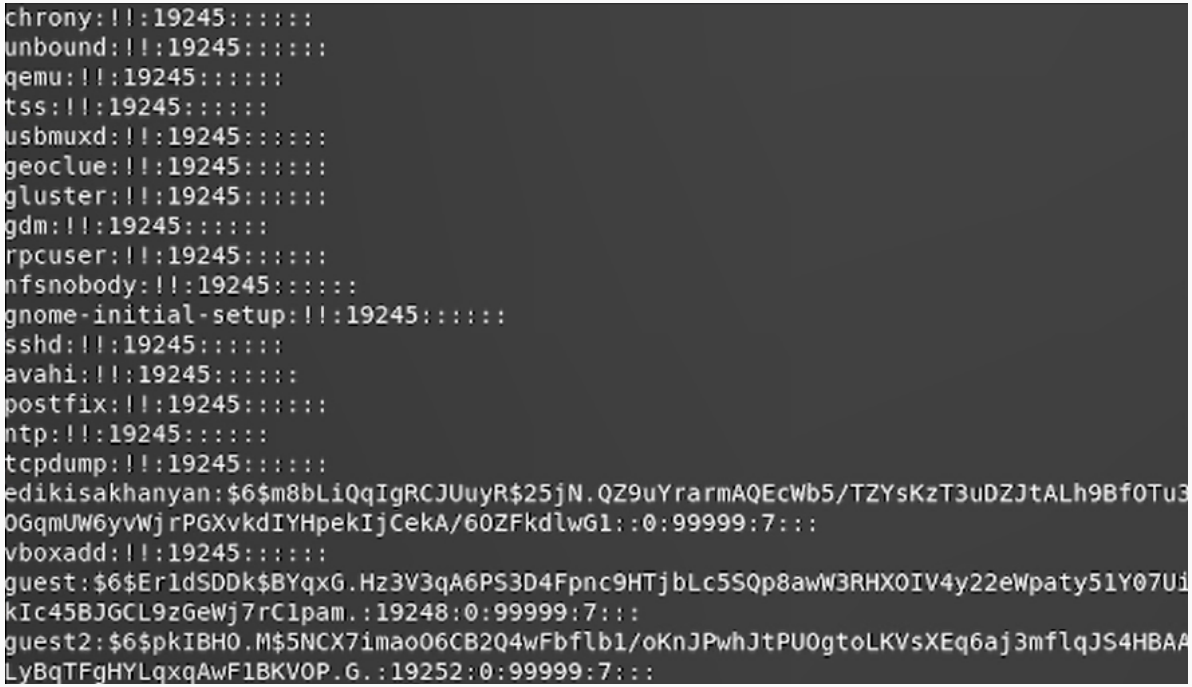

Figure 11: Программа readfile читает /etc/shadow

Исследование Sticky-бита

Исследование Sticky-бита от имени guest

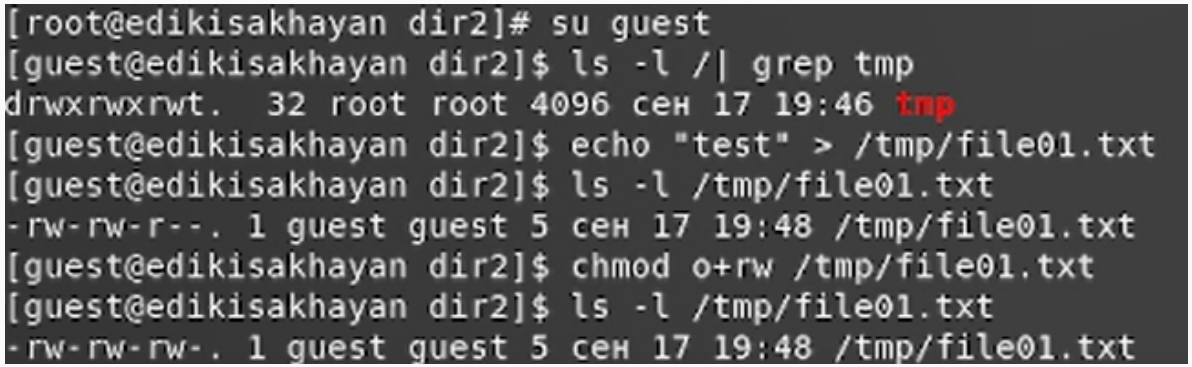

Figure 12: Исследование Sticky-бита от имени guest

Работа с file01.txt от имени guest2 при наличии Sticky-бита

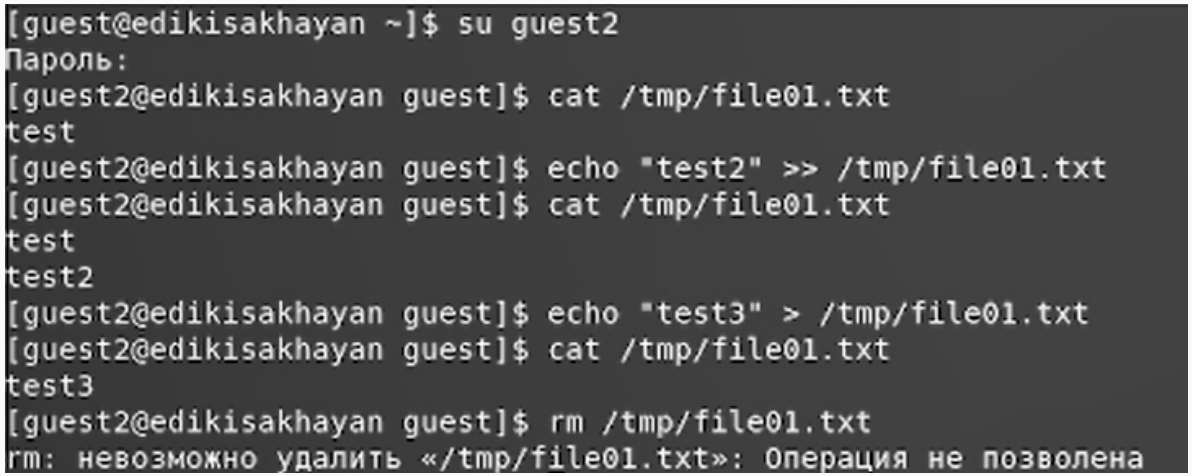

Figure 13: Работа с file01.txt от имени guest2 при наличии Sticky-бита

Снятие Sticky-бита с /tmp

```
[guest@edikisakhayan dir2]$ su
Пароль:
[root@edikisakhayan dir2]# chmod -t /tmp
[root@edikisakhayan dir2]# exit
exit
```

Figure 14: Снятие Sticky-бита с /tmp

Работа с file01.txt от имени guest2 без Sticky-бита

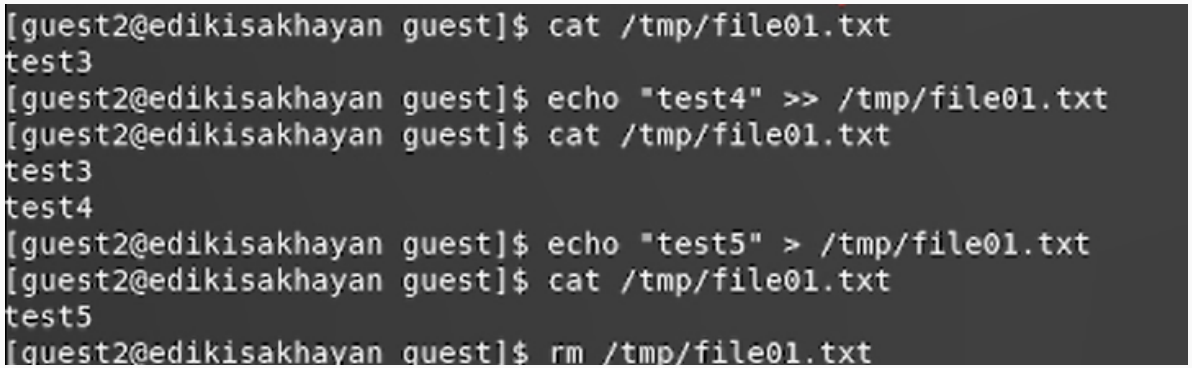

Figure 15: Работа с file01.txt от имени guest2 без Sticky-бита

Возвращение Sticky-бита на /tmp

```
[guest@edikisakhayan dir2]$ su
Пароль:
[root@edikisakhayan dir2]# chmod +t /tmp
[root@edikisakhayan dir2]# exit
exit
[guest@edikisakhayan dir2]$
```

Figure 16: Возвращение Sticky-бита на /tmp

Вывод

Вывод

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