Презентация по лабораторной работе №5

Дискреционное разграничение прав в Linux.
Исследование влияния дополнительных атрибутов

Нгуен Дык Ань

05 октября 2024

Докладчик

- Нгуен Дык Ань
- Студенческий билет: 1032215251
- Группа: НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/NguyenDucAnh0512

Цель работы

Исследовать механизм изменения идентификаторов с помощью битов SetUID и Sticky. Получить практические навыки работы в консолях с дополнительными свойствами. Рассмотреть механизм изменения идентификатора процесса пользователя, а также влияние бита Sticky на запись и удаление файлов

Выполнение работы

1. Подготовка лабораторного стенда

- Установить gcc командой “yum install gcc”.
- Отключить систему запретов до очередной перезагрузки системы командой “setenforce 0”

2. Создание программы и исследование

- Создать программу simpleid.c от имени пользователя guest, которая будет печатать на экране значения UID и GID после запуска
- Сравнить значения UID и GID
- Создать программу simpleid2.c, которая будет печатать на экране значения действительных идентификаторов
- От имени суперпользователя выполнить команды:

2. Создание программы и исследование

- “chown root:guest /home/guest/lab/simpleid2”
- “chmod u+s /home/guest/lab/simpleid2”
- Запустить simpleid2 и id, сравнить результат вывода

```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;
}
```

```
[guest@danguen lab]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

```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;
}
```

```
[root@danguen danguen]# chown root:guest /home/guest/lab/simpleid2
[root@danguen danguen]# chmod u+s /home/guest/lab/simpleid2
```

```
[guest@danguen lab]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@danguen lab]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

2. Создание программы и исследование

- Установить SetGID Бит для файла
- Проверять правильность установки новых атрибутов и смены владельца файла simpleid2
- Запустить simpleid2 и id, сравнить результат вывода

```
[root@danguen lab]# chown root:guest /home/guest/lab/simpleid2
[root@danguen lab]# chmod g+s /home/guest/lab/simpleid2
```

```
[guest@danguen lab]$ ls -l simpleid2
-rwxr-sr-x. 1 root guest 17720 Oct  5 14:57 simpleid2
```

```
[guest@danguen lab]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@danguen lab]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

2. Создание программы и исследование

- Создать и откомпилировать программу readfile.c, которая читать файл
- Сменить владельца у файла readfile.c, чтобы только суперпользователь мог прочитать его, а guest не мог
- Сменить у программы readfile владельца и установить SetUID-бит и проверять

```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;
}
```

```
[root@danguen danguen]# chown root:root /home/guest/lab/readfile.c
[root@danguen danguen]# chmod 400 /home/guest/lab/readfile.c
```

```
[guest@danguen lab]$ ls -l readfile.c
-r--------. 1 root root 402 Oct  5 00:40 readfile.c
[guest@danguen lab]$ cat readfile.c
cat: readfile.c: Permission denied
```

```
[root@danguen lab]# chown root:guest /home/guest/lab/readfile
[root@danguen lab]# chmod u+s /home/guest/lab/readfile
```

```
[guest@danguen lab]$ ls -l readfile
-rwxr-xr-x. 1 root guest 17664 Oct  5 15:06 readfile
```

```
[guest@danguen lab]$ ./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;
}
```

```
[guest@danguen lab]$ ./readfile /etc/shadow
root:$6$4Vd3He7cyG3mMYHw$yaA9iyvUza8xQTUjNbWdQ.6XwKjdlGs0EoZmDlfkJ37DLDd2K933x86
jHwOzbmlCaWCCISL8CMMOyI92f0tFC.::0:99999:7:::
bin:*:19820:0:99999:7:::
daemon:*:19820:0:99999:7:::
adm:*:19820:0:99999:7:::
lp:*:19820:0:99999:7:::
sync:*:19820:0:99999:7:::
shutdown:*:19820:0:99999:7:::
halt:*:19820:0:99999:7:::
mail:*:19820:0:99999:7:::
operator:*:19820:0:99999:7:::
games:*:19820:0:99999:7:::
ftp:*:19820:0:99999:7:::
nobody:*:19820:0:99999:7:::
systemd-coredump:!!:19970::::::
dbus:!!:19970::::::
polkitd:!!:19970::::::
avahi:!!:19970::::::
```

3. Исследование Sticky-бита

- Проверять установлен ли атрибут Sticky на директории /tmp командой “ls -l / | grep tmp”
- От имени пользователя guest создать файл file01.txt в директории /tmp со словом test
- Разрешить file01.txt прав чтения и записи для категории пользователей «все остальные»
- От пользователя guest2 (не является владельцем) попробовать прочитать файл /tmp/file01.txt

```
[root@danguen danguen]# ls -l / | grep tmp
drwxrwxrwt.  15 root root 4096 Oct  5 00:52 tmp
```

```
[guest@danguen lab]$ echo "test" > /tmp/file01.txt
[guest@danguen lab]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  5 00:54 /tmp/file01.txt
```

```
[guest@danguen lab]$ chmod o+rw /tmp/file01.txt
[guest@danguen lab]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  5 00:54 /tmp/file01.txt
```

```
[guest2@danguen danguen]$ cat /tmp/file01.txt
test
```

3. Исследование Sticky-бита

- От пользователя guest2 попробовать дозаписать в файл /tmp/file01.txt слово test2
- От пользователя guest2 попробовать удалить файл /tmp/file01.txt

```
[guest2@danguen danguen]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@danguen danguen]$ cat /tmp/file01.txt
test
```

```
[guest2@danguen danguen]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

3. Исследование Sticky-бита

- Снимать атрибут t (Sticky-бит) с директории /tmp от имени суперпользователя
- Снова от пользователя guest2 попробовать дозаписать в файл /tmp/file01.txt слово test2
- Снова от пользователя guest2 попробовать удалить файл /tmp/file01.txt
- Вернуть атрибут t на директорию /tmp от имени суперпользователя

```
[root@danguen danguen]# chmod -t /tmp
[root@danguen danguen]# exit
exit
```

```
[guest2@danguen danguen]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
```

```
[guest2@danguen danguen]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@danguen danguen]$
```

```
[root@danguen danguen]# chmod +t /tmp
[root@danguen danguen]# ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 Oct  5 15:21 tmp
```

Вывод

После лабораторной работы я получил практические навыки работы в консолях с дополнительными свойствами