Отчёт по лабораторной работе №5

Дискреционное Разграничение Прав в Linux. Исследование Влияния Дополнительных Атрибутов

Осман АлиНиколай

Содержание

1 Цель работы **5**

2 Выполнение лабораторной работы **6**

3 Выводы **14**

Список литературы **15**

Список иллюстраций

2.1 Проверка рабочее пространство 6
2.2 Создание simpleid.c 6
2.3 код программы 1 7
2.4 Вывод simpleid.c 7
2.5 simpleid2.c 8
2.6 Вывод simpleid2.c 8
2.7 сравнение simpleid2 на id 9
2.8 Программу readfile.c 10
2.9 Смена владельца файла и прав доступа 10
2.10 Попытка прочесть файл 10
2.11 Попытка 3 прочесть файл 11
2.12 Чтение файла от суперпользователя 11
2.13 Создание файла 12
2.14 изменение права доступа 12
2.15 Проверка файл на чтение, запись и удаление 12
2.16 Снятие атрибута Sticky 13
2.17 Повтор предыдущих действий 13
2.18 Изменение атрибутов 13

Список таблиц

1 Цель работы

Изучение механизмов изменения идентификатаровб 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.

2 Выполнение лабораторной работы

До начала работы проверил, что имеется средства разработки:

```
[osmanalinikolay@osmanalinikolay ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.info.gz
[osmanalinikolay@osmanalinikolay ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[osmanalinikolay@osmanalinikolay ~]$ gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/8/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Target: x86_64-redhat-linux
Configured with: ../configure --enable-bootstrap --enable-languages=c,c++,fortran,lto --prefix=/usr --man
dir=/usr/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enable-shared -
-enable-threads=posix --enable-checking=release --enable-multilib --with-system-zlib --enable-__cxa_atexi
t --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-ver
sion-only --with-linker-hash-style=gnu --enable-plugin --enable-initfini-array --with-isl --disable-libmp
x --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet -
-with-tune=generic --with-arch_32=x86-64 --build=x86_64-redhat-linux
Thread model: posix
gcc version 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)
[osmanalinikolay@osmanalinikolay ~]$ getenforce
Permissive
[osmanalinikolay@osmanalinikolay ~]$
```

Рисунок 2.1: Проверка рабочее пространство

Вошел в систему от имени пользователя guest и создал программу simpleid.c:

```
[guest@osmanalinikolay lab5]$ touch simpleid.c
[guest@osmanalinikolay lab5]$ ls
simpleid.c
[guest@osmanalinikolay lab5]$ nano simpleid.c
[guest@osmanalinikolay lab5]$ gcc simpleid.c -o simpleid
[guest@osmanalinikolay lab5]$ ./simpleid
uid=1001, dig=1001
[guest@osmanalinikolay lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfin
ed_t:s0-s0:c0.c1023
```

C++ [redacted] 1

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
```

```
int
main(){
    uid_t uid = getuid();
    gid_t gid = getgid();
    printf("uid=\%d,gid=\%d\\n", uid, gid);
    return 0;
}
```

Рисунок 2.3: код программы 1

Скомпилировал программу и запускаю ее. Она выводит идентификатор пользователя и группы:

Рисунок 2.4: Вывод simpleid.c

Создал файл simpleid2.c добавив вывод действительных идентификаторов.

C++ [redacted] 2

```
#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;
}
```

```
[guest@osmanalinikolay lab5]$ touch simpleid2.c
[guest@osmanalinikolay lab5]$ nano simpleid2.c
[guest@osmanalinikolay lab5]$ gcc simpleid2.c -o simpleid2
```

Рисунок 2.5: simpleid2.c

Скомпилировал программу и запускаю ее.

```
[guest@osmanalinikolay lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рисунок 2.6: Вывод simpleid2.c

С помощью chown изменяю владельца файла на суперпользователя, с помощью chmod изменяю права доступа

Сравнение вывода программы и команды id, наша программа вывела только ограниченное количество информации

```
[guest@osmanalinikolay lab5]$ ls -l
total 72
-rwsrwxr-x. 1 root  guest 18256 Apr 18 10:06 readfile
-rwx------. 1 root  guest   424 Apr 18 10:06 readfile.c
-rwxrwxr-x. 1 guest guest 18208 Apr 18 09:13 simpleid
-rwxrwsr-x. 1 root  guest 18256 Apr 18 09:26 simpleid2
-rw-rw-r--. 1 guest guest   319 Apr 18 09:24 simpleid2.c
-rw-rw-r--. 1 guest guest   180 Apr 18 09:12 simpleid.c
```

Рисунок 2.7: сравнение simpleid2 на id

Создал еще одну программу readfile.c

C++ [redacted] 3

```
#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@osmanalinikolay ~]# /home/guest/lab5/simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@osmanalinikolay ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
```

Рисунок 2.8: Программу readfile.c

Снова от имени суперпользователи изменил владельца файла readfile. Далее изменил права доступа так, чтобы пользователь guest не смог прочесть содержимое файла

```
#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 (arvg[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;
                                    [ Read 24 lines ]
```

Рисунок 2.9: Смена владельца файла и прав доступа

Проверка прочесть файл от имени пользователя guest. Прочесть файл не удается. Попытка прочесть тот же файл с помощью программы readfile, в ответ получаем «отказано в доступе»

```
[root@osmanalinikolay ~]# chown root:guest /home/guest/lab5/readfile.c
[root@osmanalinikolay ~]# chmod u+s /home/guest/lab5/readfile.c
[root@osmanalinikolay ~]# cat /home/guest/lab5/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);
```

Рисунок 2.10: Попытка прочесть файл

Попытка прочесть файл shadow с помощью программы, все еще получаем отказ в доступе

```
guest@osmanalinikolay lab5]$ ./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);
```

Рисунок 2.11: Попытка 3 прочесть файл

Попробовал прочесть эти же файлы от имени суперпользователя и чтение файлов было успешно

```
[guest@osmanalinikolay lab5]$ ./readfile etc/shadow
root:$6$/HHGY.d.z.zz.zz.zz
```

```
;5;9:*.arj=38;5;9:*.taz=38;5;9:*.lha=38;5;9:*.lz4=38;5;9:*.lzh=38;5;9:*.lzma=38;5;9:*.tlz=38;
5;9:*.txz=38;5;9:*.tzo=38;5;9:*.t7z=38;5;9:*.zip=38;5;9:*.z=38;5;9:*.dz=38;5;9:*.gz=38;5;9:*.
lrz=38;5;9:*.lz=38;5;9:*.lzo=38;5;9:*.xz=38;5;9:*.zst=38;5;9:*.tzst=38;5;9:*.bz2=38;5;9:*.bz=
38;5;9:*.tbz=38;5;9:*.tbz2=38;5;9:*.tz=38;5;9:*.deb=38;5;9:*.rpm=38;5;9:*.jar=38;5;9:*.war=38
;5;9:*.ear=38;5;9:*.sar=38;5;9:*.rar=38;5;9:*.alz=38;5;9:*.ace=38;5;9:*.zoo=38;5;9:*.cpio=38;
5;9:*.7z=38;5;9:*.rz=38;5;9:*.cab=38;5;9:*.wim=38;5;9:*.swm=38;5;9:*.dwm=38;5;9:*.esd=38;5;9:
*.jpg=38;5;13:*.jpeg=38;5;13:*.mjpg=38;5;13:*.mjpeg=38;5;13:*.gif=38;5;13:*.bmp=38;5;13:*.pbm
=38;5;13:*.pgm=38;5;13:*.ppm=38;5;13:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;13:*.tif=38;5;13:
*.tiff=38;5;13:*.png=38;5;13:*.svg=38;5;13:*.svgz=38;5;13:*.mng=38;5;13:*.pcx=38;5;13:*.mov=3
8;5;13:*.mpg=38;5;13:*.mpeg=38;5;13:*.m2v=38;5;13:*.mkv=38;5;13:*.webm=38;5;13:*.ogm=38;5;13:
*.mp4=38;5;13:*.m4v=38;5;13:*.mp4v=38;5;13:*.vob=38;5;13:*.qt=38;5;13:*.nuv=38;5;13:*.wmv=38;
5;13:*.asf=38;5;13:*.rm=38;5;13:*.rmvb=38;5;13:*.flc=38;5;13:*.avi=38;5;13:*.fli=38;5;13:*.fl
v=38;5;13:*.gl=38;5;13:*.dl=38;5;13:*.xcf=38;5;13:*.xwd=38;5;13:*.yuv=38;5;13:*.cgm=38;5;13:*
.emf=38;5;13:*.ogv=38;5;13:*.ogx=38;5;13:*.aac=38;5;45:*.au=38;5;45:*.flac=38;5;45:*.m4a=38;5
;45:*.mid=38;5;45:*.midi=38;5;45:*.mka=38;5;45:*.mp3=38;5;45:*.mpc=38;5;45:*.ogg=38;5;45:*.ra
=38;5;45:*.wav=38;5;45:*.oga=38;5;45:*.opus=38;5;45:*.spx=38;5;45:*.xspf=38;5;45:XDG_MENU_PRE
FIX=gnome-LANG=en_US.UTF-8GDM_LANG=en_US.UTF-8HISTCONTROL=ignoredupsDISPLAY=:0HOSTNAME=osmana
linikolayCOLORTERM=truecolorUSERNAME=osmanalinikolayXDG_VTNR=2which_declare=declare -fXDG_SES
SION_ID=2USER=guestDESKTOP_SESSION=gnomeWAYLAND_DISPLAY=wayland-0GNOME_TERMINAL_SCREEN=/org/g
nome/Terminal/screen/4bc84649_be70_46f5_b491_526f358f28ddPWD=/home/guest/lab5SSH_ASKPASS=/usr
/libexec/openssh/gnome-ssh-askpassHOME=/home/guestXDG_SESSION_TYPE=waylandXDG_DATA_DIRS=/home
/guest/.local/share/flatpak/exports/share:/home/osmanalinikolay/.local/share/flatpak/exports/
share:/var/lib/flatpak/exports/share:/usr/local/share/:/usr/share/XDG_SESSION_DESKTOP=gnomeGJ
S_DEBUG_OUTPUT=stderrMAIL=/var/spool/mail/osmanalinikolayTERM=xterm-256colorSHELL=/bin/bashVT
E_VERSION=5204QT_IM_MODULE=ibusXMODIFIERS=@im=ibusXDG_CURRENT_DESKTOP=GNOMEGNOME_TERMINAL_SER
VICE=:1.74SHLVL=3XDG_SEAT=seat0GDMSESSION=gnomeGNOME_DESKTOP_SESSION_ID=this-is-deprecatedLOG
```

Рисунок 2.13: Создание файла

Добавляю права на чтение и запись для других пользователей

```
[guest@osmanalinikolay ~]$ echo "test" > /tmp/file01.txt
[guest@osmanalinikolay ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Apr 18 10:30 /tmp/file01.txt
```

Рисунок 2.14: изменение права доступа

Вхожу в систему от имени пользователя guest2, от его имени могу прочитать файл file01.txt, но перезаписать информацию в нем не могу. Также невозможно добавить в файл file01.txt новую информацию от имени пользователя guest2. Когда попробовал удалить файл, снова получила отказ.

```
[guest@osmanalinikolay ~]$ chmod o+rw /tmp/file01.txt
[guest@osmanalinikolay ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Apr 18 10:30 /tmp/file01.txt
```

Рисунок 2.15: Проверка файл на чтение, запись и удаление

От имени суперпользователя снял с директории атрибут Sticky.

```
[guest@osmanalinikolay ~]$ su - guest2
Password:
[guest2@osmanalinikolay ~]$ cat /tmp/file01.txt
test
[guest2@osmanalinikolay ~]$ echo "test2" > /tmp/file01.txt
[guest2@osmanalinikolay ~]$ echo "test3" >> /tmp/file01.txt
[guest2@osmanalinikolay ~]$ cat /tmp/file01.txt
test2
test3
[guest2@osmanalinikolay ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Рисунок 2.16: Снятие атрибута Sticky

Проверил, что атрибут действительно снят и выполнен повтор предыдущих действий. По результатам без Sticky-бита запись в файл и дозапись в файл осталась невозможной

```
[guest2@osmanalinikolay ~]$ su -
Password:
[root@osmanalinikolay ~]# chmod -t /tmp
[root@osmanalinikolay ~]# exit
logout
```

Рисунок 2.17: Повтор предыдущих действий

Возвращение директории tmp атрибута t от имени суперпользователя

```
[guest@osmanalinikolay ~]$ su - guest2
Password:
[guest2@osmanalinikolay ~]$ cat /tmp/file01.txt
test
[guest2@osmanalinikolay ~]$ echo "test2" > /tmp/file01.txt
[guest2@osmanalinikolay ~]$ echo "test3" >> /tmp/file01.txt
[guest2@osmanalinikolay ~]$ cat /tmp/file01.txt
test2
test3
[guest2@osmanalinikolay ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Рисунок 2.18: Изменение атрибутов

3 Выводы

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

Список литературы