Презентация по лабораторной работе №5

Информационная безопасность

Байрамгельдыев Довлетмурат

5 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Байрамгельдыев Довлетмурат
- студент 4 курса группы НФИбд-01-20
- ст. б. 1032207470
- Российский университет дружбы народов
- 1032207470@pfur.ru

Вводная часть

Актуальность

- Обеспечение безопасности

Цели и задачи

- Приобретение практических навыков работы в консоли с дополнительными атрибутами файлов
- Изучение механизмов смены идентификатора процессов пользователей
- Изучение SetUID-, SetGID- и Sticky-битов

Материалы и методы

- Веб-сервис `GitHub` для работы с репозиториями
- Программа для виртуализации ОС `VirtualBox`
- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `docx`
- Автоматизация процесса создания: `Makefile`

Ход работы

Написание программы 1

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;
}
```

Запуск программы 1

```
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
```

```
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

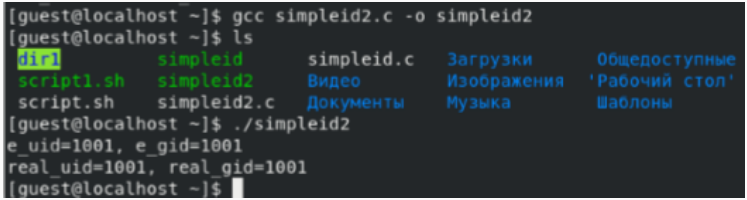
Модификация программы

simpleid.c × 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;
}
```

Запуск модифицированной программы



Изменение владельца файла

```
[guest@localhost ~]$ su
Пароль:
```

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

```
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Написание программы 3

simpleid.c × simpleid2.c × **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;
}
```

Изменение прав доступа

```
[root@localhost guest]# chown root:guest /home/guest/readfile.c
[root@localhost guest]# chmod 700 /home/guest/readfile.c
```

```
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
```

Попытка чтения, изменения и удаления файла

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

```
[guest2@localhost guest]$ echo "test3" > /tmp/file01.txt
[guest2@localhost guest]$
```

```
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

Снятие Sticky-бита

```
[guest2@localhost guest]$ su
Пароль:
[root@localhost guest]# chmod -t /tmp
```

```
[root@localhost guest]# exit
exit
```

Повторная попытка чтения, записи и удаления файла

```
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
test2
[guest2@localhost guest]$ echo "test3" > /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test3
[guest2@localhost guest]$ rm /tmp/file01.txt
[guest2@localhost guest]$ ls /tmp
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-bolt.service-rjjegM
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-colord.service-JRG69N
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-fwupd.service-MNRVCT
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-geoclue.service-TbVhfc
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-ModemManager.service-NJ6cCp
systemd-private-8553bbdafd5a4298b486bab82e5b76a9-rtkit-daemon.service-ZVzhLm
tracker-extract-files.1001
```

Результаты

Результаты работы

- Получены навыки работы с дополнительными атрибутами файлов
- Усовершенствованы навыки работы с механизмами смены владельца
- Рассмотрены принципы работы SetUID-, SetGID- и Sticky-битов-