fd

1976年4月11日 星期四　　下午1:05

```
~  ssh fd@pwnable.kr -p2222
fd@pwnable.kr's password:
 ____  __    __  ____    ____  ____   _        __      __  _  ____
|    \|  |__|  ||    \  /    ||    \ | |      /  ]    |  |/ ]|    \
|  o  )  |  |  ||  _  ||  o  ||  o  )| |     /  [_     |  ' / |  D  )
|   _/|  |  |  ||  |  ||     ||     || |___ |    _]    |    \ |    /
|  |  |  `  '  ||  |  ||  _  ||  O  ||     ||   [_  __ |     \|    \
|  |   \      / |  |  ||  |  ||     ||     ||     ||  ||  .  ||  .  \
|__|    \_/\_/  |__|__||__|__||_____||_____||_____||__||__|\_||__|\_|

- Site admin : daehee87.kr@gmail.com
- IRC : irc.netgarage.org:6667 / #pwnable.kr
- Simply type "irssi" command to join IRC now
- files under /tmp can be erased anytime. make your directory under /tmp
- to use peda, issue `source /usr/share/peda/peda.py` in gdb terminal
Last login: Wed Apr 10 20:30:38 2019 from 183.230.42.68
fd@ubuntu:~$
```

先连接到目标服务器。

查看文件

```
fd@ubuntu:~$ ls -la
total 40
drwxr-x---  5 root   fd   4096 Oct 26  2016 .
drwxr-xr-x 93 root   root 4096 Oct 10 22:56 ..
d---------  2 root   root 4096 Jun 12  2014 .bash_history
-rw-------  1 root   root  128 Oct 26  2016 .gdb_history
dr-xr-xr-x  2 root   root 4096 Dec 19  2016 .irssi
drwxr-xr-x  2 root   root 4096 Oct 23  2016 .pwntools-cache
-r-sr-x---  1 fd_pwn fd   7322 Jun 11  2014 fd
-rw-r--r--  1 root   root  418 Jun 11  2014 fd.c
-r--r-----  1 fd_pwn root   50 Jun 11  2014 flag
fd@ubuntu:~$
```

发现有一个可执行文件，源码，以及flag。

查看源码

```
fd@ubuntu:~$ cat fd.c
#include <stdio.h>
#include <stdlib.h>
```

```
#include <string.h>
char buf[32];
int main(int argc, char* argv[], char* envp[]){
        if(argc<2){
                printf("pass argv[1] a number\n");
                return 0;
        }
        int fd = atoi( argv[1] ) - 0x1234;
        int len = 0;
        len = read(fd, buf, 32);
        if(!strcmp("LETMEWIN\n", buf)){
                printf("good job :)\n");
                system("/bin/cat flag");
                exit(0);
        }
        printf("learn about Linux file IO\n");
        return 0;

}

fd@ubuntu:~$
```

我们通过阅读源码可知，我们只需使buf中为"LETMEWIN\n"，这样就可以执行/bin/flag，也就可以获得flag。

此时我们应该

查看read函数的使用方法。

```
READ(2)                                   Linux Programmer's Manual                                   READ(2)

NAME
       read - read from a file descriptor

SYNOPSIS
       #include <unistd.h>

       ssize_t read(int fd, void *buf, size_t count);

DESCRIPTION
       read() attempts to read up to count bytes from file descriptor fd into the buffer starting at buf.

       On files that support seeking, the read operation commences at the current file offset, and the file offset is incremented by
       the number of bytes read.  If the current file offset is at or past the end of file, no bytes are read,  and  read()  returns
       zero.

       If  count  is  zero, read() may detect the errors described below.  In the absence of any errors, or if read() does not check
       for errors, a read() with a count of 0 returns zero and has no other effects.

       If count is greater than SSIZE_MAX, the result is unspecified.

RETURN VALUE
       On success, the number of bytes read is returned (zero indicates end of file), and the file position is advanced by this num-
       ber.   It  is  not an error if this number is smaller than the number of bytes requested; this may happen for example because
       fewer bytes are actually available right now (maybe because we were close to end-of-file, or because we are  reading  from  a
       pipe, or from a terminal), or because read() was interrupted by a signal.  See also NOTES.

       On error, -1 is returned, and errno is set appropriately.  In this case, it is left unspecified whether the file position (if
       any) changes.
```

通过man命令我们可以获得read函数的使用方法，参数，以及返回值类型。

如果fd为0的话，程序将从stdin读入数据放入到buf，这正是我们想要的。

程序中有对fd赋值，只需使fd为零。0x1234转换为十进制为4660。通过man命令查询到atoi函数的作用是把string装换为int。

下面我们就来pwn：

至此我们获取了flag。

2019/4/11