

pwnable.kr-cmd1-Writeup

转载

[baikeng3674](#) 于 2017-02-11 14:56:00 发布 42 收藏

文章标签: [运维](#) [c/c++](#)

原文链接: <http://www.cnblogs.com/WangAoBo/p/6389160.html>

版权

MarkdownPad Document

pwnable.kr-cmd1-Writeup

这道题挺有意思，这里详细的记录一下：

- 首先还是ssh远程登录，ls -l查看文件，然后cat cmd1.c读C代码如下：

```
1 #include <stdio.h>
2 #include <string.h>
3
4 int filter(char* cmd){
5     int r=0;
6     r += strstr(cmd, "flag")!=0;
7     r += strstr(cmd, "sh")!=0;
8     r += strstr(cmd, "tmp")!=0;
9     return r;
10 }
11 int main(int argc, char* argv[], char** envp){
12     putenv("PATH=/fuckyouverymuch");
13     if(filter(argv[1])) return 0;
14     system( argv[1] );
15     return 0;
16 }
```

- 先查到主函数main的第三个参数envp和环境变量有关；
- putenv()函数是改变环境变量的，因此更改了环境变量后，惯用的ls, cat等命令都不能直接使用，但我们通过完整路径来使用，如/bin/cat；
- strstr(str1, str2)函数，当str2包含在str1中，返回str2在str1中的索引；否则返回0；
- 然后分析r += strstr(cmd, "flag")!=0, 根据C语言中+=运算符从右向左读的规则，该行代码可以分解为：

```
int tmp = strstr(cmd,"flag")!=0 ? 0 : 1;
r += tmp;
```

- 则有：

其中，argv[1] == "/bin/cat f*"中使用了通配符来避免出现关键字字符串flag；

- 传递参数如下：

则flag即为 **mommy now I get what PATH environment is for :)**
2017-2-11 14:52;38

转载于:<https://www.cnblogs.com/WangAoBo/p/6389160.html>