pwnable.kr-cmd1-Writeup

转载

m626i46i 于 2017-02-15 12:07:53 发布
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：

```
#include <stdio.h>
#include <string.h>

int filter(char* cmd){
    int r=0;
    r += strstr(cmd, "flag")!=0;
    r += strstr(cmd, "sh")!=0;
    r += strstr(cmd, "tmp")!=0;
    return r;
}
int main(int argc, char* argv[], char** envp){
    putenv("PATH=/fuckyouverymuch");
    if(filter(argv[1])) return 0;
    system( argv[1] );
    return 0;
}
```

- 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** 从又向左读的规则，该行代码可以分解为：

```
int tmp = strstr(cmd,"flag")? 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