闭关学pwn第一天——了解数据结构中的栈（文末彩蛋）

原创

mid2dog 于 2019-11-21 16:49:16 发布 609 收藏 8

分类专栏： pwn入门 文章标签： 栈溢出 pwn ctf 萌新 入门

前言

看pwn的writeup，发现都看不懂= =
那些大佬的wp看起来跟参考答案是略没什么区别啊（雾）！！
然后决定从最基本的学起来，每天补一点知识，一边闭关一边刷题。
听说栈溢出挺简单的（当我没说----by三小时以后的我）,那就先从学栈开始吧。

了解栈

上百度
注：按顺序食用效果更佳

1.生动形象说明了栈

超生动，超级形象

2.简单的介绍栈

这里面有个地方**设栈的最大长度为size，栈满不可入栈（上溢）[top=size-1]**
我理解是top是从[0]开始的，所以装满了顶部指针会是top=size-1
而后面的出栈操作也验证了这个理解
只有栈顶元素才可出栈，栈空不可出栈
栈空条件：top=-1；
所以top确实是从0开始的

3.栈的三种含义

在pwn里用到的栈溢出应该是第三种（雾）

4.百度百科栈

这里大致看一下概念就好了
然后百度百科里有一句话没怎么看懂
在i386机器中，栈顶由称为esp的寄存器进行定位。压栈的操作使得栈顶的地址减小，弹出的操作使得栈顶的地址增大
为什么压栈的操作会使栈顶地址减小啊，压栈不是往上放东西吗，那地址不就多了吗…
然后各种百度，这个问题见5

5.操作系统中栈与堆的理解

对刚才提出的问题解释很透彻了，因为它是向下生长的，是倒过来的，所以压栈地址会减小，弹出地址会增大。这篇文章里提到的ESP和EBP寄存器不懂，阻碍了理解，继续百度

6.ESP寄存器与EBP寄存器

看完了以后再回头看5，现在就很好理解了，ebp为基指针，然后要调用函数的时候把esp往下放，用完了再来个（move esp，ebp）也就是把ebp的值赋给esp，这样下方的空间就又都收回来了，好玩。

7.关于栈的理解

最后再看看别人的理解巩固一下。说实话这篇看起来讲的详细，但还是很烧脑……

栈溢出

开始学栈溢出，资料如下
手把手教你栈溢出从入门到放弃（上）
手把手教你栈溢出从入门到放弃（下）

一.判断栈溢出条件

1.程序要有向栈内写入数据的行为。
2.程序并不限制写入数据的长度。

二.攻击方法

在溢出数据内包含攻击指令的内容或地址。

三.知识补充

对不懂的地方进行百度知识补充
EIP & EBP & ESP
这里有一句话说的非常棒：
其实我们对这个只需要知道三个指针是什么就可以，可能对我们以后学习栈溢出的问题以及看栈这方面的书籍有些帮助。当有人再给你说EIP,ESP,EBP的时候，你不能一头雾水，那你水平就显得洼了许多。其实不知道我们照样可以编程，因为我们是C级别的程序员，而不是ASM级别的程序员

而这里面也介绍了栈溢出，可以先看这里面的栈溢出再去看“**手把手教你栈溢出从入门到放弃（上）**”

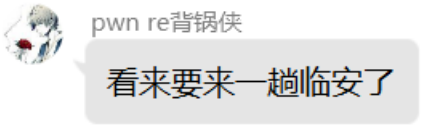
四.开始学习

这里先从栈溢出的上篇开始学习，因为上篇介绍了栈溢出的原理和两种覆盖地址的方法。这两种方法都需要操作系统关闭内存布局随机化（ASLR）并且shellcode 需要程序调用栈有可执行权限。下篇讲的就是克制ASLR的方法，今天是pwn第一天，先学上篇好咯，明天看下篇。

坐等南邮的nctf出pwn中关于栈溢出的题目来练练手[手动滑稽]

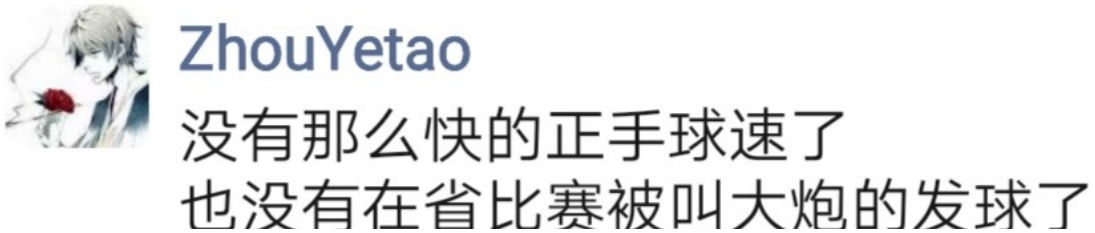
总结

万事开头难，但总得开个头吧
希望能有闭关学pwn第二天



说起开头难emmm…（最近很危险，似乎有人想开我头）
丝毫不慌。

因为……



还有的就是一身的伤
都特么快残废了😭😭😭

昨天

漂亮啊，网球干的漂亮！网球兄弟，nice！