看雪一位牛人的腾讯面试

原创

买成衣的女程序员 于 2012-02-25 23:15:07 发布 4111 收藏 2
文章标签： 面试 腾讯 电话 算法 汇编 游戏

在一个月前，正当准备回家的时候，突然看到**兄招人的信息，由于无心准备找工作，所以也没怎么打算投递简历。后来随便聊聊，才知道是腾讯招人，在和**兄聊得比较愉快，所以就投了一份简历。**兄看后，便说通过电话面试。于是就电话面试了，主要是面试了以下几个问题：

1、_STDCALL的参数压栈方式，堆栈平衡方式

这个比较基础，是从右到左依次压入，CALL内平衡

2、C语言里wsprintf参数的压栈方式，为什么

这个也比较基础，就是从右到左依次压入，CALL外平衡。为什么，其实当时我没想起来，**兄告诉我了，是因为wsprintf的参数是可变的，当他告诉我的时候，我突然想起来了。。

3、PE里面物理和文件地址的转换

这个也比较基址，我自觉得对PE还算了解，还算熟悉，所以关于va,rva等这个没有问题。

4、常见的注入方式

我当时说了，注入的方式很多，常用的有Ipk、pe感染方式(也就是导出函数方式)，输入法等等。。。

5、OD常用的快捷方式

我平时比较习惯于用鼠标，因为我发现窗口最大化不是很好。当然常用的还是知道，哈哈，shift+2,f2,f7,8,9，alt+e等等。

6、IDA的结构使用

这个我只会操作，所以使用，电话里面我没说得很好。

7、如何分析一个数据的方法：

我答：通过输出字符串，导出函数或者CE工具，定位内存地址，通过IDA静态分析结合 OD动态调试，很快就可以找到想要的了。

7、目前游戏常见的保护方式，及其破解方式

我说了NP、HS、GPK等保护的特性，及破解方式。在这里我就不一一细说了，有兴趣的朋友，可以私下交流。

这个电话面试后，hr来电通知我说电话面试通过，要赴公司面试。其实不管3Q大战还是以前，腾讯给我的感觉还是挺好的，很多人都说腾讯喜欢抄袭别人创意，但是站在一个软件工作从业者的角度，我觉得还是挺配服腾讯，因为我看到了它很多产品有自己的创新，特别在用户友好方面做得比较不错。所以内心还是比较喜欢腾讯的，于是决定以后在那边发展，在网上更新了简历，令自己很开心的是，得到了腾讯互娱内部（至少有3位朋友），包括华为，迅雷等其他公司的邀请，但是说实在的，其他公司可能和我自己喜欢的方向不太匹配，所以我委婉的拒绝了。心想能去腾讯从事逆向方面也行，于是订好机票过去了。

今天下午2：30面试，第一轮面试就是**兄面试，

1、第一个问题就是进程间通信的问题，比如一个外挂注入游戏后的dll,如何和面界exe进行通信。

这个就是内存映射的问题，当然我还向**兄画图详细讲解了我曾经分析一个游戏的程序,engin.dll如何同ui.exe进行通信交互的。

有必需要的朋友，大可以一起交流。涉及到外挂的隙疑我就不在这里发了。

2、一个函数如 funA(int a,int b,……)；如果在这个函数内部打出CALL调用后的地址，也就是调用完函数EIP的地址。

这个当时我一下没明白，因为以前做hook的时候，都是用函数指针，对了，他要求不能用汇编和shell等方式，所以一时明白，**兄提示了一下，让我想想栈的情况，我马就明白了。

```
int * dwTmp = &a;
 int dwEip = *(int *)(dwTmp -4);
```

那么这个dwEip就是funA调用后返回eip的值。

3、写一个数组排序

这个就不说了，写了一个很简单的冒泡排序之后其他的一些无关紧要的问题。

之后就是**兄的老大面试:

1、离职的原因

******

2、注入的方式

******电话面试的时候说了，我又说了一下。

3、PE的常见区段，一个全局变量在哪个区段

text,data,rdata……

一个全局变量在data段，不时我是这么答的，

4、软件系统的设计

由于老大看到我在之前的公司做系统设计，这也是我悲据的开始，当时正在这个时候腾讯在拖台球桌很吵，也不知道这个老大听到我讲的没，要是没听到我这里再写一下。

设计分为数据库设计和系统设计，数据设计包括概念设计和物理设计。系统包括概要设计，详细设计。这个地方答得比较简单，然后又一直纠结于如何设好一个页面，页面与页面之间的交互，页面设计的原则是什么。我实在不想回答这些问题，但是没办法。我根据我的经验，就答：保持用户友好性，简单方便原则。我不知道有没有答错，有这方面经验的朋友告诉我。

5、设计模式观察者模式，单件模式

说实在的，我从事软件开发的时候，面向对象还是不错的，但是这二年来一直在弄汇编、内存方面的东西，所以忘得差不多了，直接回答观察者模式忘了，单件模式这个是最简单的，我回答了，也不知道老大听到了没，因为很吵。

6、STL方面的

这个我当时直接回答，不会。其实我会使用，你让我说，我确实说不出来。所以心想过掉就算了。

7、其他一些我也听清楚他到底在问什么样，因为旁边有台球桌不停的在弄，实在没听清楚再之后是等待啊等待，近一个多小时后，**兄老大的老大终于出现了：

上来弄了一个很不好的气氛，一上来提问,在上一家什么公司，做什么游戏的保护？

因为担心有其他的考虑，所以我当时请求就说，能不能不说公司和做的产品的情况，老大不愧是老大，就说：那这样我们就终止面试。无奈还是把上一家公司的情况给说了，内疚啊，唉。然后就纠接着私服的问题，我不知道老大曾经是否弄过私服，问：别人拿不到服务端，分析别人的服务端的干嘛。。总之就是一直纠接这个问题。。。。

后来就问我反外挂有些一些保护，我不知道是指思路还是具体的方式，因为老大的声音很小，并且旁边也很吵，我就说：进程保护，反调，内存段CRC效验，关键算法VM等。

之后老大就丢下二个题目，让我手写代码，然后又离开了，这一去又是近1个小时，这二个题目是：
1、1个字符串如12345（这个字符串是十六进制的）用汇编转传化成十进制。
　这个题其实不难，但是我确实不想用手写代码，不怎么习惯。写了一下伪代码。可惜后面老大也没怎么看吧。
　说一下我自己的思路，若是有好的思路，也欢迎朋友们说说，
　取得12345这个字符串的首地址，然后逐个字符取出来，按照如下来做就行了:
　1*10(4次方)+2*10(3)+3*10(2)+4*10(1)+5*10(0)

2、用C/C++手写九宫图算法。
　类似这样的算法，实在不会，如实说了不会。

大约等了1个小时后，老大终于出现了，直接问有没有什么给他加分的？
　我的回答的是，我只对逆向调试分析感兴趣，兴趣使然。
然后最后一个问题问我：能否接受同第三方公司签约，不以腾讯公司的签约。
　偶一听很反感，因为我对外包不感兴趣，所以我直接拒绝。当然我也知道意味着什么。

　很奇怪反外挂岗位，这次面试为什么不去讨论一下进程、线程的保护，反调技术，内存效验，堆栈检验，底层驱动更是一个都不提，难道TX只关注应用层保护，底层放弃了？更多的是在排序、九宫图算法这块，唉。

　虽然**兄最后电话我，说帮我推到安全中心去，我说算了，还是很感谢**兄的邀请，可能本人能力确实有待提高。像腾讯公司应该招的是顶级的牛人。偶等小菜实在不该去献丑啊。以前分析过NP、HS，GPK等游戏大概有十多款，以后我得多逆向分析一下腾讯的游戏，向TX大牛们学习一下算法，提高一下自己的算法水平。我想从技术方面研究，应该不算为违法吧。

　这次面试很感激**兄的邀请，让我有机会体验国内最大互联网公司的面试，从中我也学习到了一些东西，同时也知道自身的短处，更可贵的是遇到了看雪的另一位牛人，一起吃了饭，聚了聚挺开心的，他顺利通过了，以后一定向他也多学习。以后一定多发一些文章或者经验贴，我羞愧至今一篇精华贴都没有。
同时本人也顺便发一个求职贴，哈哈，不知道是否违规了，简单的自我介绍一下：
　我工作了5年，熟练.net,c/c++,会win32,mfc编程，熟悉汇编编程，熟悉内存结构，对操作系统有一定的了解，对外挂、木马、私服相同技术比较熟悉。常用的调试工具od,ida,windbg等不用说了，还算比较熟练，呵呵。

　特别调试分析这块经验比较丰富，有逆向分析这方面工作岗位的，可以站内联系一下我。谢谢(同时注明：谢绝外挂、私服、木马开发。因为本人胆小)。

　现在虽然身在异乡，不能回家团聚，也不后悔，正好可以静心再整理一下最近几年自己从事过的技术工作，潜心低调修行，最后再一次感谢看雪**兄，有机会一定再聚聚。