

**汇编语言与逆向技术课程实验报告**

**实验八：REChallenge**

****

学 院 网络空间安全学院

专 业 信息安全

学 号 2313546

姓 名 蒋枘言

班 级 信息安全班

一、实验目的

1.熟悉反编译工具Binary Ninja；

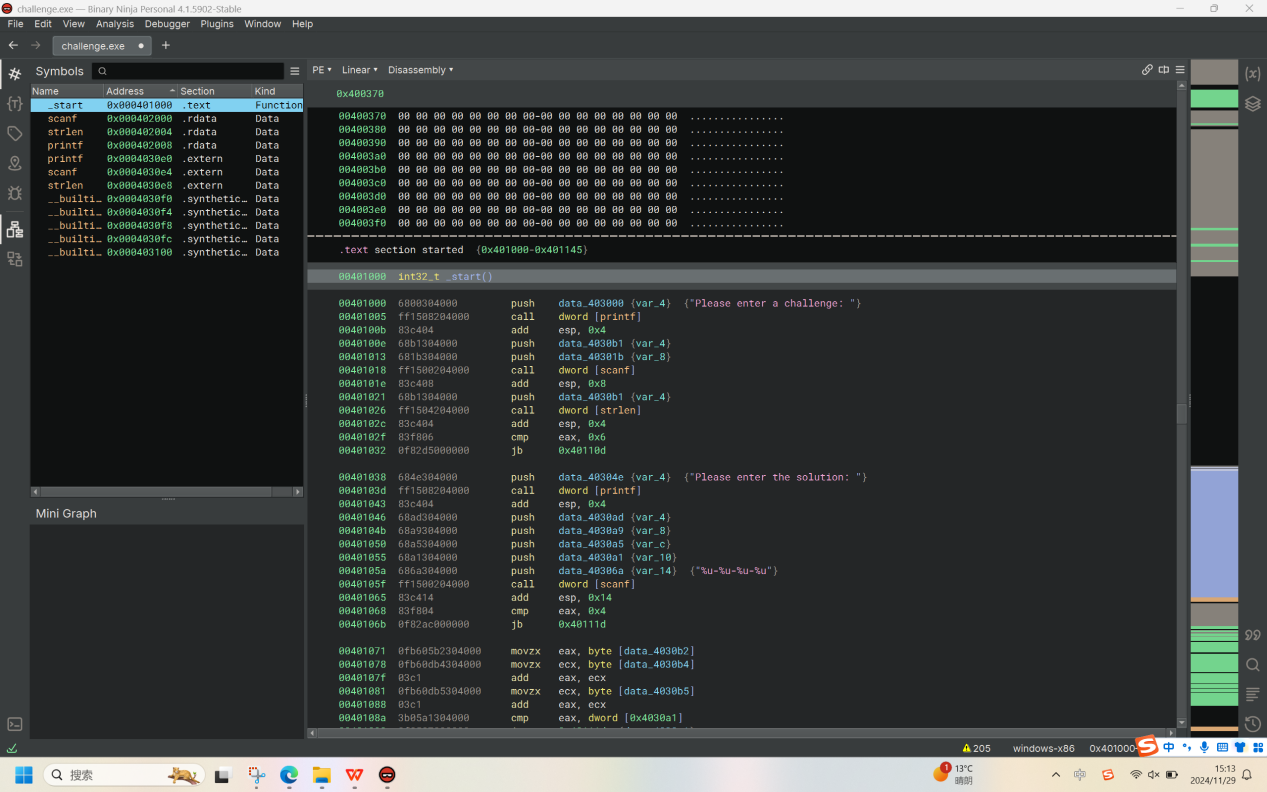
2.熟悉反汇编代码的逆向分析过程；

3.掌握反汇编语言中的数学计算、数据结构、条件判断、分支结构的识别和逆向分析。

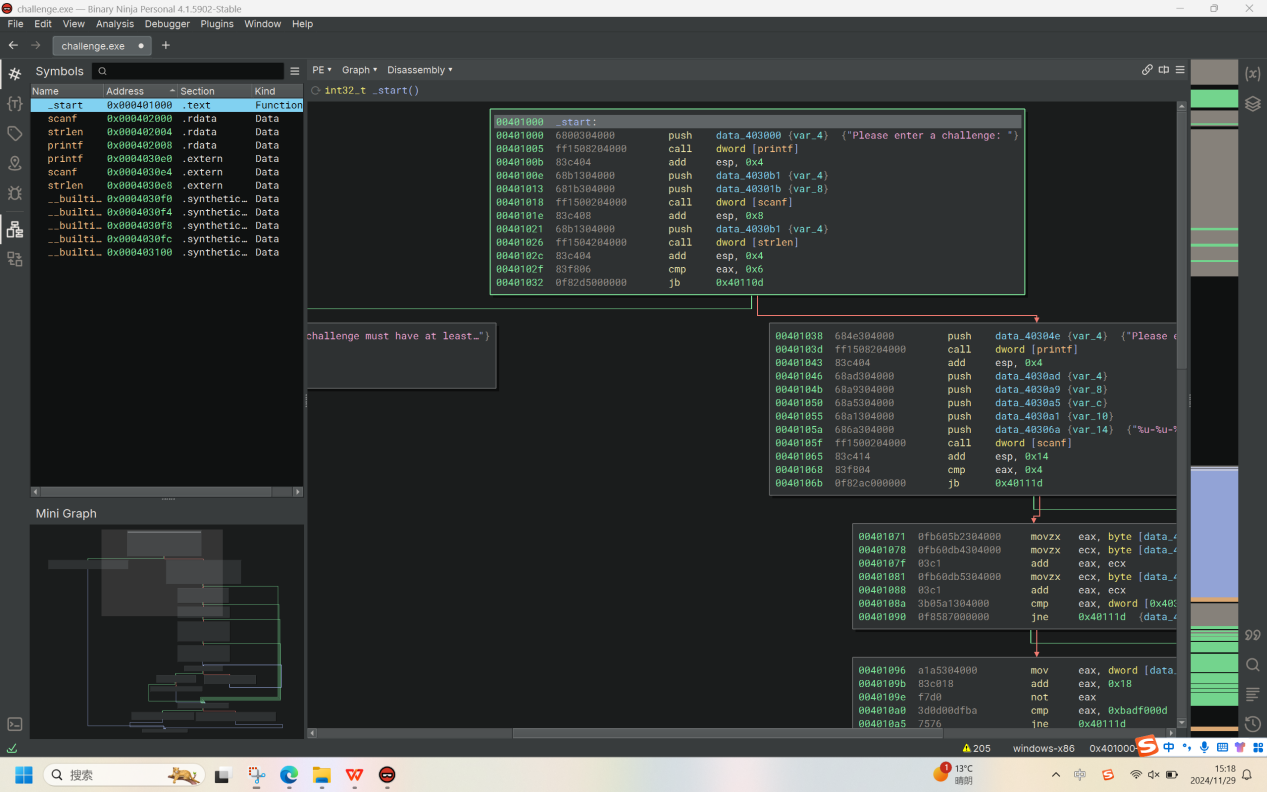
二、打开文件

使用Binary Ninja打开待分析的exe文件：challenge.exe。

反汇编代码如下图所示：



图形化视窗如下图所示：

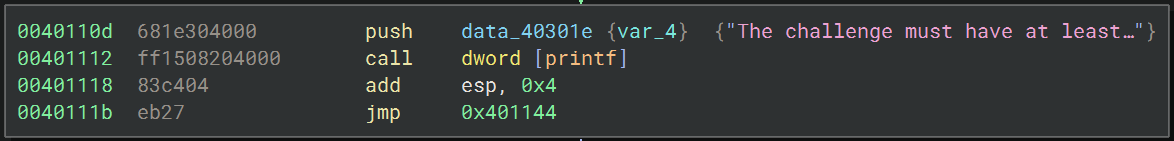


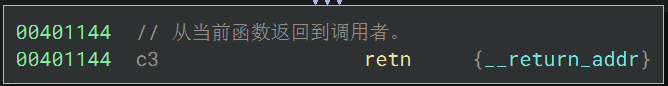
三、逆向分析过程**（代码逐行解释详见截图）**

**1.输入判断**

这是程序.text节的入口点位置（00401000处）。这一小部分的主要作用是提示用户输入一个字符串challenge，并且对输入的字符串challenge进行判断。如果字符串challenge的长度小于6，则跳转到0040110d位置。

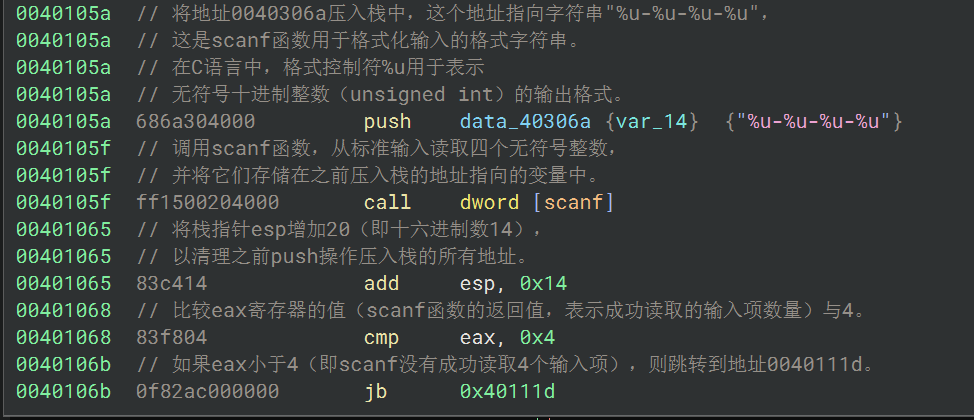
**2.输入的长度不符合要求**

****0040110d位置输出字符串“The challenge must have at least 6 characters”，随后跳转到位置0401144。

**3.程序结束**

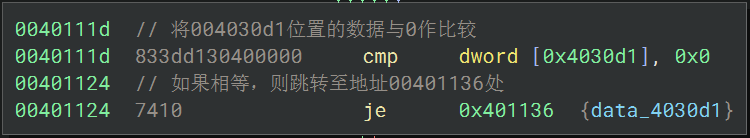
位置0401144是程序的结束位置。即如果字符串challenge的长度小于6，在输出了字符串“The challenge must have at least 6 characters”之后，程序结束。

**4.输入的长度符合要求**

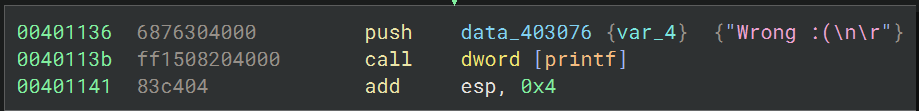
若输入的长度符合要求，首先会输出字符串“Please enter the solution: ”来引导用户输入答案。答案是一个形如“%u-%u-%u-%u”的字符串，“%u”是C语言的一个格式控制符，用于表示无符号十进制整数（unsigned int）的输出格式。

随后判断输入的个数是否为4。若小于4，则跳转到地址0040111d。

**5.输入的个数不符合要求**

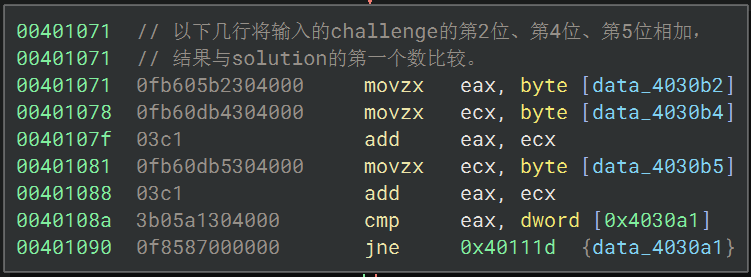


首先将004030d1位置的数据与0作比较。可以发现该位置的数据本来就被初始化为了0，故相等。于是就会跳转到00401136位置。

随后输出字符串“Wrong :(”，代表答案错误。

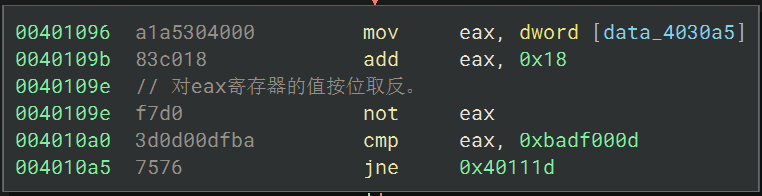
按顺序执行00401144，即**第3点**所讲的程序结束。

**6.输入的个数符合要求——solution第1个数判断**



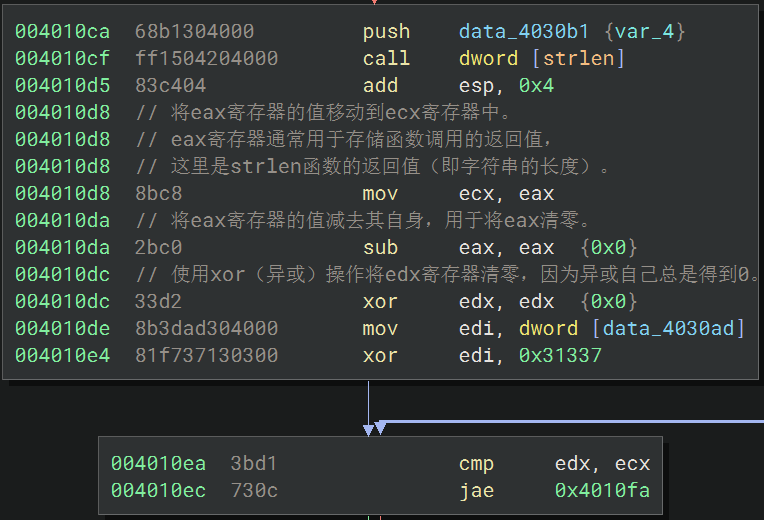
将challenge的第2、4、5位相加，结果与solution的第1个数比较。若不相等，则跳转到地址0040111d，后续和**第5点**相同。

**7.输入的个数符合要求——solution第2个数判断**

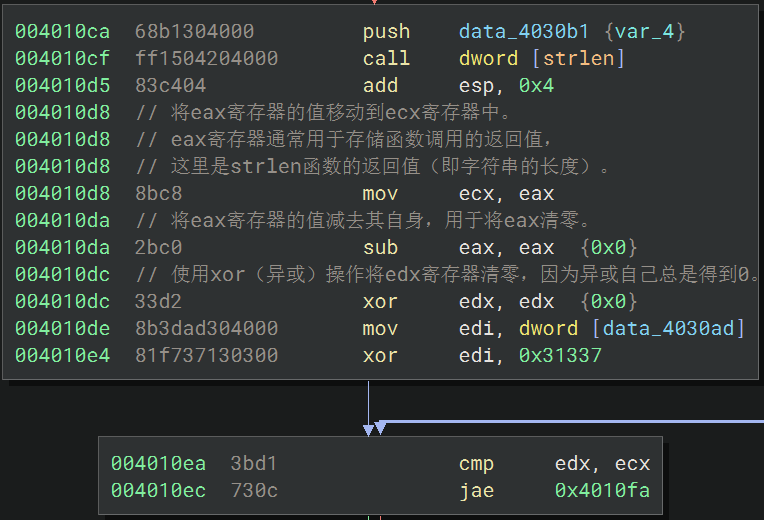
将solution的第2个数加上24（即十六进制数18），然后按位取反，与十六进制数badf0000d作比较。若不相等，则跳转到地址0040111d，后续和**第5点**相同。

**8.输入的个数符合要求——solution第3个数判断**

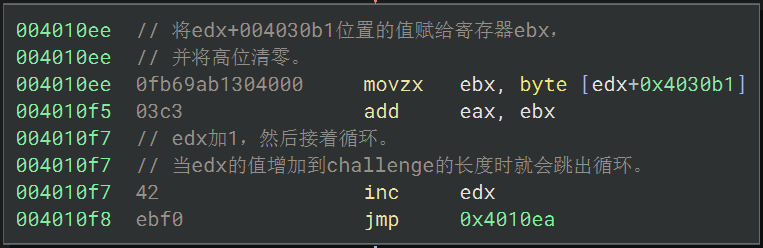
将solution的第3个数****除以十六进制数c48，得到的商与challenge的第1、3位相乘的结果作比较。若不相等，则跳转到地址0040111d，后续和**第5点**相同。

**9.输入的个数符合要求——solution第4个数判断**

**（第10点跳转位置）**

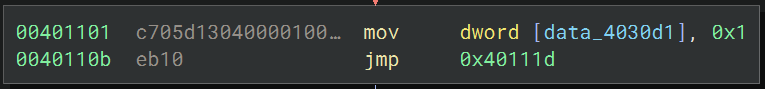
将challenge的长度与edx寄存器的值（被初始化为0）作比较，若edx寄存器的值大于等于challenge的长度，则跳转至地址004010fa。

**10.edx寄存器的值小于challenge的长度**

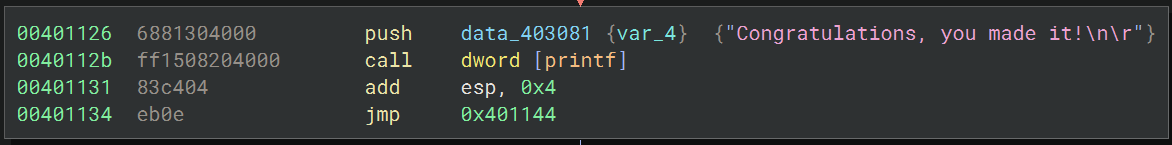
此部分是一个循环（循环到**第9点**中间），每次循环将edx加1，循环结束后就将字符串challenge的每一位相加，值储存在eax中。

**11.edx寄存器的值大于等于challenge的长度**

将edi寄存器的值减去十六进制数7b后与eax作比较。若不等，则跳转至0040111d位置，进入**第5点**。

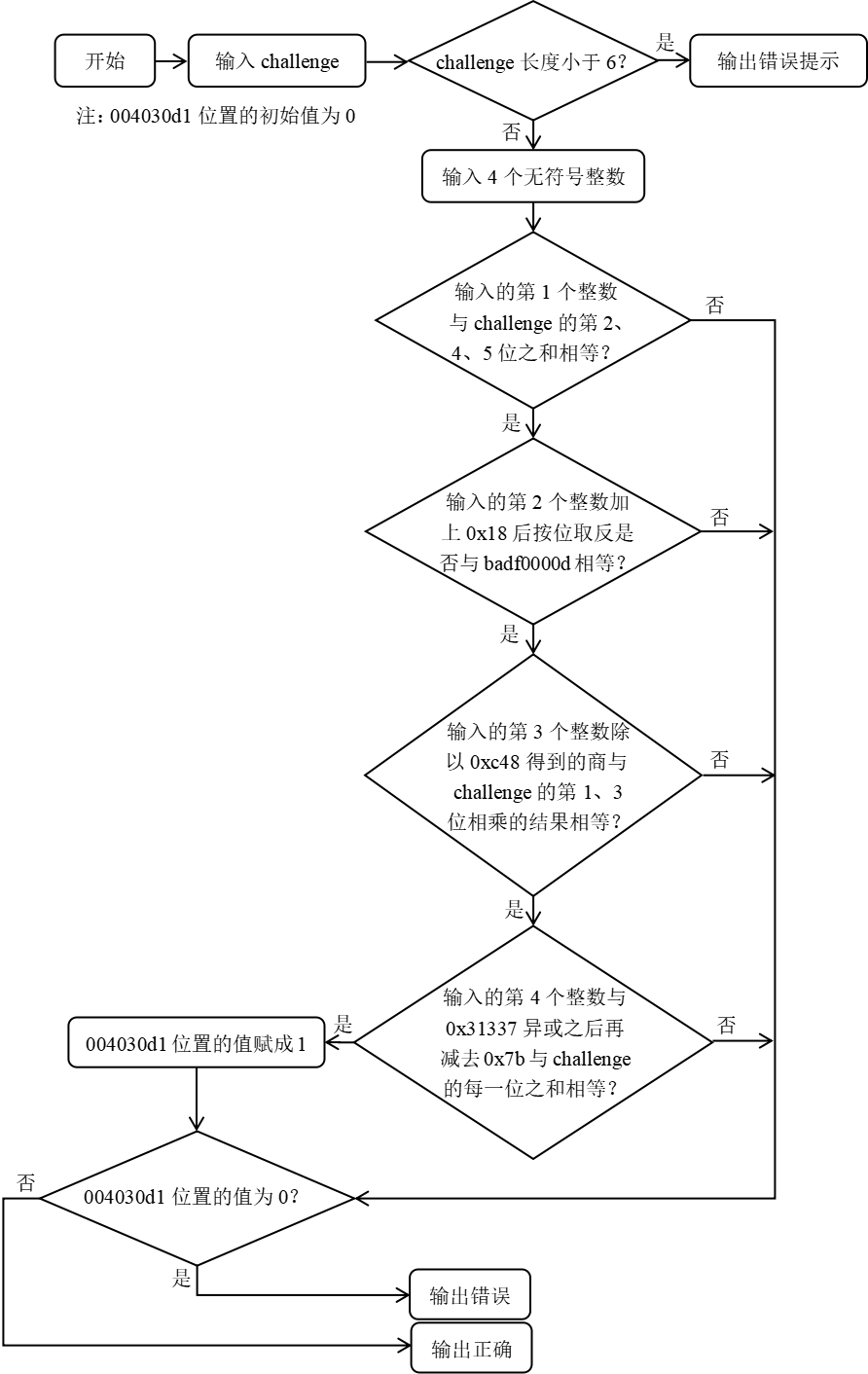
若相等，则将004030d1位置的值修改成1，再跳转至0040111d位置，进入**第5点**。

**12.solution正确**

由于004030d1位置的值被修改成1，不与0相等，所以跳转到000401126位置。输出“Congratulations, you made it!”，代表solution正确。随后跳转至00401144位置，进入**第3点**，程序结束。

四、逆向分析流程图

（见下页）



五、结果验证

输入challenge为114514，输入solution为151-1159790554-8010912-201372，结果正确。

