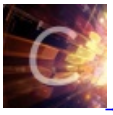
2实验吧逆向

原创

卦星 于 2016-06-09 00:01:10 发布 1545 收藏
分类专栏： 逆向学习记录 文章标签： 实验吧 babycrack



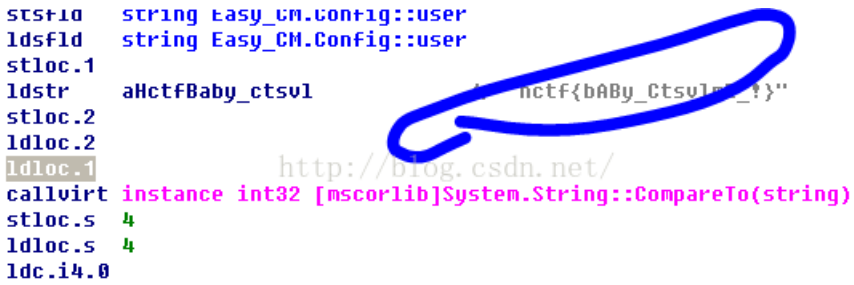
1.1 概述

随着对安全的逐渐深入的学习，在接触部分linux知识的过程中，认识了不少CTF的大神，这些大神有不少是顶级赛棍，奈何非科班出身的计算机基础差的要命，只能一点一点积累和记录了
这一系列文章仅仅是自己的学习记录，写博客督促自己不断学习的，其实如果查资料，并没有啥有价值的东西
本次记录的是我的第二次逆向题目，来自

1.2 实验吧的“babycrack”？开始逆向

1.2.1 使用PEID查看是否存在壳，（略）

1.2.2 导入IDA一看，是一个.net程序，比较坑爹（这个真不懂，以前写过一点MFC，不过，后来都忘了，硬着头皮点下去）



投机取巧了，不好意思，这个真没分析出来逻辑，但是字符串就在那放着！
我也明白为啥是babycrack了

1.3实验吧的“阿拉神灯”？开始逆向

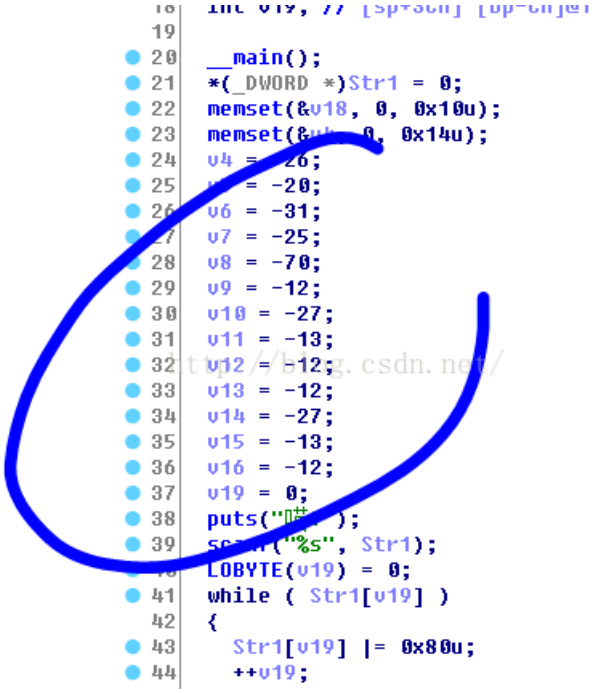
```
aForm1:                                 // DATA XREF: WindowsApplication1.Form1__InitializeComponent+290
    unicode <Form1>,0
asc_1134:                               // DATA XREF: WindowsApplication1.Form1__InitializeComponent+29B
                                        // WindowsApplication1.Form1__Button1_Click+26↑o ...
    unicode <通关密语>,0
aZhimakaimen@20:                        // DATA XREF: WindowsApplication1.Form1__Button1_Click+12↑o
    unicode <zhimakaimen@2011>,0
asc_1160:                               // DATA XREF: WindowsApplication1.Form1__Button1_Click+20↑o
    unicode <通关密语正确！>,0
asc_1170:                               // DATA XREF: WindowsApplication1.Form1__Button1_Click:loc_7B3↑o
    unicode <通关密语错误！>,0
aWindowsapplica:                        // DATA XREF: WindowsApplication1.My.Resources.Resources__get_Re
    unicode <WindowsApplication1.Resources>,0
aM:                                     // DATA XREF: WindowsApplication1.My.Resources.Resources__get_m+
    unicode <m>,0
```


字符串中有明文！

1.4实验吧的“just click”？开始逆向
使用IDA折腾一上午，后来才明白，其实c#可以更简单的ILSpy工具

```
// rev4.MainWindow
private void btn_Checker(int para)
{
    int[] array = new int[]
    {
        0,
        1,
        3,
        4,
        2,
        1,
        2,
        3,
        4
    };
    bool flag = this.hit < 8;
    if (flag)
    {
        int num = this.hit;
        this.hit = num + 1;
    }
    else
    {
        base.Close();
    }
    bool flag2 = this.first;
    if (flag2)
    {
        this.tb1.Text = "";
        this.first = false;
    }
    bool flag3 = array[this.hit] == para;
    if (flag3)
    {
        int num = this.correct;
        this.correct = num + 1;
    }
```


1.4 100000
拖入ida 逆向出算法，结果如下



正向是和0x80u求|.反向应该是求& 0x7f得到结果，