python 重定向 ctf_CTF逆向--.NET与Python篇

weixin_39982537 于 2020-12-10 08:24:38 发布 29 收藏
文章标签： python 重定向 ctf

下面就可以写脚本获取flag

import base64,binascii from Crypto.Cipher import AES key = 'pctf2016pctf2016pctf2016pctf2016' result = 'x/nzolo0TTlyrElSd4AP1spCzlhSWJXeNbY81SjPgmk=' after_encrypt = binascii.b2a_hex(base64.b64decode(result)) a = AES.new(key) flag = a.decrypt(after_encrypt.decode('hex')) print flag

Flag：PCTF{Dot_Net_UnPack3r_yoo}

FindKey

这是一道pyc逆向，直接百度pyc在线逆向，找到相应的网站后上传需要逆向的pyc文件，接下来就能得到源码，如下所示

#!/usr/bin/env python # encoding: utf-8 # 访问 http://tool.lu/pyc/ 查看更多信息 import sys lookup = [196,153,149,206,17,221,10,217,167,18,36,135,103,61,111,31,92,152,21,228,105,191,173,41,2,245,23,144, 1,246,89,178,182,119,38,85,48,226,165,241,166,214,71,90,151,3,109,169,150,224,69,156,158,57,181,29, 200,37,51,252,227,93,65,82,66,80,170,77,49,177,81,94,202,107,25,73,148,98,129,231,212,14,84,121,174, 171,64,180,233,74,140,242,75,104,253,44,39,87,86,27,68,22,55,76,35,248,96,5,56,20,161,213,238,220,72, 100,247,8,63,249,145,243,155,222,122,32,43,186,0,102,216,126,15,42,115,138,240,147,229,204,117,223,141 159,131,232,124,254,60,116,46,113,79,16,128,6,251,40,205,137,199,83,54,188,19,184,201,110,255,26,91,21 132,160,168,154,185,183,244,78,33,123,28,59,12,210,218,47,163,215,209,108,235,237,118,101,24,234,106,1 88,9,136,95,30,193,176,225,198,197,194,239,134,162,192,11,70,58,187,50,67,236,230,13,99,190,208,207,7,5 219,203,62,114,127,125,164,179,175,112,172,250,133,130,52,189,97,146,34,157,120,195,45,4,142,139] pwda = [188,155,11,58,251,208,204,202,150,120,206,237,114,92,126,6,42] pwdb = [53,222,230,35,67,248,226,216,17,209,32,2,181,200,171,60,108] flag = raw_input('Input your Key:').strip() if len(flag) != 17: print 'Wrong Key!!' sys.exit(1) flag = flag[::-1] for i in range(0, len(flag)): if ord(flag[i]) + pwda[i] & 255 != lookup[i + pwdb[i]]: print 'Wrong Key!!' sys.exit(1) print 'Congratulations!!'

很简单，将其的代码复制下来就可得到flag，脚本如下所示

lookup = [196,153,149,206,17,221,10,217,167,18,36,135,103,61,111,31,92,152,21,228,105,191,173,41,2,245,23,144, 1,246,89,178,182,119,38,85,48,226,165,241,166,214,71,90,151,3,109,169,150,224,69,156,158,57,181,29, 200,37,51,252,227,93,65,82,66,80,170,77,49,177,81,94,202,107,25,73,148,98,129,231,212,14,84,121,174, 171,64,180,233,74,140,242,75,104,253,44,39,87,86,27,68,22,55,76,35,248,96,5,56,20,161,213,238,220,72, 100,247,8,63,249,145,243,155,222,122,32,43,186,0,102,216,126,15,42,115,138,240,147,229,204,117,223,141 159,131,232,124,254,60,116,46,113,79,16,128,6,251,40,205,137,199,83,54,188,19,184,201,110,255,26,91,21 132,160,168,154,185,183,244,78,33,123,28,59,12,210,218,47,163,215,209,108,235,237,118,101,24,234,106,1 88,9,136,95,30,193,176,225,198,197,194,239,134,162,192,11,70,58,187,50,67,236,230,13,99,190,208,207,7,5 219,203,62,114,127,125,164,179,175,112,172,250,133,130,52,189,97,146,34,157,120,195,45,4,142,139] pwda = [188,155,11,58,251,208,204,202,150,120,206,237,114,92,126,6,42] pwdb = [53,222,230,35,67,248,226,216,17,209,32,2,181,200,171,60,108]flag = "" for i in range(17): flag += chr(lookup[i+pwdb[i]] - pwda[i]&255) print flag[::-1]

Flag：PCTF{PyC_Cr4ck3r}

Login

首先查壳

没壳，拖进IDA，F12查看字符串，发现里面出现了python的标志

按理来说一般的c程序是不会出现python的，但是这里却出现了大量的Py前缀，这说明什么呢，说明这个exe实际上是一个python转exe的程序(你问我为什么会知道？因为我之前在HXBCTF征题的时候就出了道Python转exe的题打算坑一坑人/ω\),在网上下一个pyinstxtractor.py就可将其解压，然后查看解压后的文件夹

首先看到有一堆API的dll，不管它，然后还看到一个Python35.dll，查一下壳，发现是UPX加壳的，使用脱壳机脱掉后，丢进IDA里查看，点击F12查看字符串，一大堆字符串-_-||，尝试搜索一下flag，然后发现了这个

查看引用后来到了这个函数

就这样来到了核心代码的位置，这里可以看到if (v3 != (v4 ^ byte_1E253040[v3]))这个if判断是关键判断，只有当其正确，整个while循环才会执行到输出Congratulation处而V4就是用户输入的Password，因此就可以写一个脚本来得出flag

a = [0x50 ,0x78 ,0x76 ,0x6B ,0x34 ,0x6B ,0x59 ,0x63 ,0x49 ,0x56 ,0x6C ,0x4A ,0x53 ,0x65 ,0x4F ,0x3F] count = 0 flag = '' for i in range(len(a)): for i in range(33,127): if i^a[count] == count: flag += chr(i) count += 1 break print flag

这里的a就是上面代码中的byte_1E253040数组

Flag：Pyth0n_dA_fA_hA0

长按二维码向我转账

受苹果公司新规定影响，微信 iOS 版的赞赏功能被关闭，可通过二维码转账支持公众号。

阅读

好看

已推荐到看一看

你的朋友可以在“发现”-“看一看”看到你认为好看的文章。

已取消，“好看”想法已同步删除

已推荐到看一看

和朋友分享想法

最多200字，当前共字

发送

已发送

朋友将在看一看看到

确定

分享你的想法...

取消

分享想法到看一看

确定

最多200字，当前共字

发送中

网络异常，请稍后重试

微信扫一扫

关注该公众号