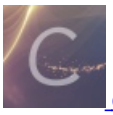
XCTF-Reverse-ExerciseArea-009-writeup

原创

y4ung 于 2019-08-05 19:05:05 发布 4030 收藏

分类专栏： ctf 文章标签： ctf ReverseEngineering



0x00 介绍

本题是xctf攻防世界中Reverse的新手第九题。题目来源： `NJUPT CTF 2017`

给了一个python经过编译后得到的字节文件Py.pyc，需要对该二进制文件进行逆向分析，找到flag

实验环境：IDA Pro 7.0，gdb

0x01 解题过程

1.1 文件分析

这是一个用Python2.7写的程序。修改文件权限为可执行，运行该文件。需要输入flag

```
root@kali:~/hzy/ctf-learning# file Py.pyc
Py.pyc: python 2.7 byte-compiled
root@kali:~/hzy/ctf-learning# chmod +x Py.pyc
root@kali:~/hzy/ctf-learning# ./Py.pyc
Input flag:
abcdefg
wrong
root@kali:~/hzy/ctf-learning#
```

1.2 逆向分析

使用python反汇编的在线工具：在线pyc,pyo反编译python反编译对 `Py.pyc` 文件进行反汇编，得到以下结果：

```python
#! /usr/bin/env python 2.7 (62211)
#coding=utf-8
# Compiled at: 2017-06-02 21:20:43
#Powered by BugScaner
#http://tools.bugscaner.com/
#如果觉得不错,请分享给你朋友使用吧!
import base64

def encode(message):
    s = ''
    for i in message:  # 对于用户输入的每个字符
        x = ord(i) ^ 32  # 取字符的ASCII码，跟32异或
        x = x + 16  # 加上16
        s += chr(x)  # 转成字符

    return base64.b64encode(s)


correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
flag = ''
print 'Input flag:'
flag = raw_input()
if encode(flag) == correct:
    print 'correct'
else:
    print 'wrong'
```

用户输入的flag经过encode函数编码，得到的结果与`XlNkVmtUI1MgXWBZXCFeKY+AaXNt`字符串一样才能通过

因此，要写出encode函数的逆过程

Tips: 异或的逆运算为

```
若a^b=c
则a=b^c
```

因此，编写以下的代码进行解码

```python
import base64

def decode(encode_str):
    s = base64.b64decode(encode_str)
    print(s)
    s = "".join(map(chr, s))
    res = ""

    for each in s:
        x = ord(each)
        x = x - 16
        x = x ^ 32
        x = chr(x)
        res = res + x

    return res


if __name__ == "__main__":
    encode_str = "XlNkVmtUI1MgXWBZXCFeKY+AaXNt"
    res = decode(encode_str)

    print(res)
```

flag为：`nctf{d3c0mpil1n9_PyC}`