XDCTF 部分Writeup

原创

whym1 于 2017-10-03 10:40:03 发布 418 收藏

分类专栏： Writeup 文章标签： xdctf writeup

Crypto

基础为王

分析数据包分离手动分离出两个png

两个图片xor后，得到flag

基础之base64

一开始以为是写脚本批量解base64，得到一个c程序，运行拿到helloworld不对，
后来网上搜了一下，base64隐写
直接谷歌拿到脚本,贴上代码

```
# -*- coding: cp936 -*-
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('encode_code.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 =  ''.join(stegb64.decode('base64').encode('base64').split())
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
        print ''.join([chr(int(bin_str[i:i + 8], 2)) for i in xrange(0, len(bin_str), 8)]) #8位一组
```

运行拿到flag

Misc

水表

文件对比，

hex(36) = 0x20 + 0xdb = hex(48) + 0xCF == 0xFF

那么data= hex(100) checkdigit= 0xff - data

然后组合，大写即为flag

邮箱

说到邮箱先想到的是163邮箱，试了一下

```
strings -a blog.pcapng | grep @163.com
```

在搜索结果后竟然真发现一个邮箱

提交，即为flag

勒索病毒

数据包分理出一个7z格式压缩的压缩包，打开得到一个vbs脚本，猜vbs脚本加载必须要wscript.exe的支持，于是提交，即为flag

智能变电站

数据包分析，根据protocal排序，一个一个protocal，追踪tcp流，根据题目提示，16个报告控制块被占满，找到了

数字前的即为ID，拿到flag

Android

Crack Me

运行后发现，

参数为xianRE:(,之后调用decrypt函数，而decrypt函数试缺失的，那么就得寻找真正的函数，这时候解压出来的另一个文件就有作用了，分离出一个rar解压得到origin.jar，打开jar文件，找到真正的decrypt函数，

编译用AndroidStudio编译这段安卓代码，拿到对应的smali文件，替换smali重打包即可拿到flag

工作验证码

易知道，关键函数一定在encrypt函数，和verify函数，两者皆为native函数，IDA打开

观察encrypt函数，发现先与一个数组进行异或，然后再进行base64加密，

而verify函数则是，一个简单的比较是否相等，直接上脚本

```
import base64
  pas = 'My_S3cr3t_P@$$W0rD'+ '\0'
  flag = base64.b64decode('KxU+NEhUEFVBaWB4HUAyVgZ3ZnlLamAHAUUHR20zJlk=')
  input = ''
  for i in xrange(0,len(flag)):
      input += chr(ord(flag[i]) ^ ord(pas[i % 0x13]))
  print input
```

运行拿到flag