ctf解密图片得到flag_CTF从入门到进（fang）阶(qi)之MISC

原创

weixin_39819576 于 2020-12-20 04:35:18 发布 2621 收藏 4
文章标签： ctf解密图片得到flag

原标题：CTF从入门到进(fang)阶(qi)之MISC

本文用到的题目链接：https://share.weiyun.com/1bd2cdb2d5e8276204a74efbf0530529

0x01 背景

CTF竞赛是安全圈喜闻乐见的竞赛模式，对于培养网络安全技术人才起到了很重要的作用。CTF起源于1996年DEFCON全球黑客大会，是Capture The Flag的简称。经过多年的发展，CTF这种比赛形式已经日益成熟。

CTF注重动手技能，深厚的理论功底厚积薄发，技术的卓越是建立在无数次训练的基础上，那么我们来看看有哪些不错的平台可以来用于比赛训练。

一般线上初选采用传统的夺旗赛模式，也就是在题目中设置一些标识，解题的目的就是为了找到标识并提交。通常包含的题目类型包括MISC、CRYPTO、PWN、REVERSE、WEB等。本文主要介绍MISC

•MISC(Miscellaneous)类型，即安全杂项，题目或涉及流量分析、电子取证、人肉搜索、数据分析等等。

0x02 MISC介绍

MISC，中文即杂项，包括隐写，数据还原，脑洞、社会工程、与信息安全相关的大数据等。

竞赛过程中解MISC时会涉及到各种脑洞，各种花式技巧，主要考察选手的快速理解、学习能力以及日常知识积累的广度、深度。

MISC这一块并不像PWNREVERSE等需要深厚的理论基础，所以我们直接从经典题目开始入手。

0x03 说明

0x04部分为WP，作为给小伙伴们提供结题思路之用，如果想获得好的训练效果，请先不要看0x04部分。前往文章开篇给出的链接或点击“阅读原文”下载题目自己先动手试试。

0x04 CTF仿真题WP

1.紧急报文

密文都由ADFGX，百度一下，发现有个ADFGX密码

密码表如图

对应着解密即可

FA XX DD AG FF XG FD XG DD DG GA XF FA

flagxidianctf

提交：flag_Xd{hSh_ctf:flagxidianctf}

2.flag.xls先介绍最简单的方法

直接仍在winhex中然后查找flag关键字即可

别的方法也是半斤八两，因为打开xls它要密码，所以我们就用notepad或者notepad++打开都行，在搜索flag就行了

3.图片里的动漫

一张图片而已，果断拉到kali里binwalk

看到了ZIP

于是后缀改为.zip打开，得到flag.rar,需要密码，再次binwalk

发现.JPEG,于是改格式为.jpeg,打开发现是七龙珠的图片

题目提示是小写英文字母，七龙珠的英文是dragon ball,提示发现错误

考虑到图片是倒着的，所以答案也是倒着的，即逆序，得到答案

CTF{llabnogard}

4.Canon

下载后解压是一段mp3和一个压缩文件，压缩文件打不开先放着，我们先处理mp3 。

misc肯定会涉及到隐写，处理mp3的隐写一般使用mp3Stego,但是处理时需要密码，试试用标题Canon

打开文件夹，发现

打开txt，里面的就是前面的压缩文件的解压密码

解压后里面有个txt,目测是,但是这么长的让你解密是不合理的，所以考虑可能是某种类型的某件缺了些代码，补上后再按照相应的格式打开就行了 。

txt文件提示我们是png格式，所以直接后缀改为.png用winhex打开看看，发现没有明显的文件头 。

所以我们给它添加，这里直接用Python来，顺便生成最后的图片

import

```
def foo():
f=open('C:UsershaseeDownloadsmimimizippic_png.txt').read()
fsave=open('pic.png','wb')
addHeader="89 50 4E 47 0D 0A 1A 0A".replace(' ','').decode('hex')
fsave.write(addHeader)
fsave.write(.b64decode(f))
fsave.close()
pass
if name == 'main':
foo()
print 'ok'
pass
```

打开生成后的图片得到答案

当然，非要解密也行，解密后把看上去干净点的代码复制到word里查找CTF就得到答案了

5.ROT-13变身了

rot-13作为置换暗码的一种都是数字怎么可能，所以应该想到ascii

题目提示回旋13，我们-13就行了

python中的chr可以自动转换，我们由此跑python

????表示为未知，给我们的MD5也查不出来，所以只能自己爆破了，爆破的思路大概就是：

？作为ASCII的可见字符，范围在32-126，有95种可能，四个？？？？所以有95^4中可能，每种排列出来后再进行MD验证

由此思想来跑PYHTON

得出答案

6.解码磁带

只有字符'o'和下划线''，不免让我们想起二进制，只有0和1，却能表示所有信息，所以我们尝试用0，1替换o和

而究竟0对于o还是_呢？我们有例子可以得到

跑Python的思路是这样子的，换成二进制后再转换成ascii，然后相应解码即可，也可以参考这张图片

直接用二进制对应字母

python结果如下：

按照格式提交即可

7.功夫秘籍

下载来的是一个压缩包，打开它。。。我的天，居然打不开。扔到winhex看看，发现是png

本来想直接改成png的，但是想到改了之后还是要winhex,干脆直接搜索key,flag等关键字，找到了

目测，解码

目测栅栏，解码

提交时只需要提交{}里面的内容就行了

8.WTF?

打开一看一堆乱七八糟的东西，不过拉到最下面发现有=，解之

得到01的组合

数了一下有65536 = 256*256

正方形是吧

那么尝试组个正方形出来

作图的话processing挺好用

扫一扫就出来了

9.社交网络

下载来的压缩文件需要密码，爆破之

解压后得到文件，右键查看属性，得到flag

10.有趣的文件

最前面的8位是地址，不用管，后面的应该是文件头，百度afbc 1c27

这个任务太繁重了，本来还想这放在winhex里面手工的，这里直接Python吧

```
def revStr(s):
news=""
for i in xrange(0,len(s),4):
news+=s[i+2:i+4]
news+=s[i:i+2]
return news
def foo():
f=open('funfile')
s="377a"
for line in f:
s+=revStr(line.strip()[8:].replace(' ',""))
fsave=open('fun.7z','wb')
fsave.write(s.decode('hex'))
fsave.close()
pass
if name == 'main':
foo()
print 'finished'
```

自动生成fun.7z压缩文件，解压后是一张阿狸的图片，拖进winhex看看，发现疑似flag的加密过的

复制后解码就行了

0x05 结语

看到这儿，小伙伴们是不是觉得MISC很有意思呢，由于MISC的类型比较多，难免挂一漏万，不过我还是尽可能多地给小伙伴提供各种花式姿(知)势(识)。

MISC之路，漫漫其修远兮，且行且珍惜。

预告：下一篇CTF系列将会继续介绍MISC题目的其他类型，同时总结MISC技巧并提供MISC所涉及到的工具及其用法演示。

如果看完这一篇还不过瘾的话可以去合天官网做实验继续学习哦。

http://www.hetianlab.com/cour.do?w=1&c=C9d6c0ca797abec20161101170431000001

别忘了投稿哟！！！

合天公众号开启原创投稿啦！！！

大家有好的技术原创文章。

欢迎投稿至邮箱：edu@heetian.com；

合天会根据文章的时效、新颖、文笔、实用等多方面评判给予100元-500元不等的稿费哟。

有才能的你快来投稿吧！

合天网安实验室

网址 : www.hetianlab.com

电话：4006-123-731

责任编辑：