HackTheBox-blackSquare

原创

galaxy3000 于 2022-02-25 13:27:05 发布 2717 收藏

分类专栏： # Misc 文章标签： CTF hackthebox writeup Misc 网络安全

本文链接：https://blog.csdn.net/galaxy3000/article/details/123130809

Misc 专栏收录该内容

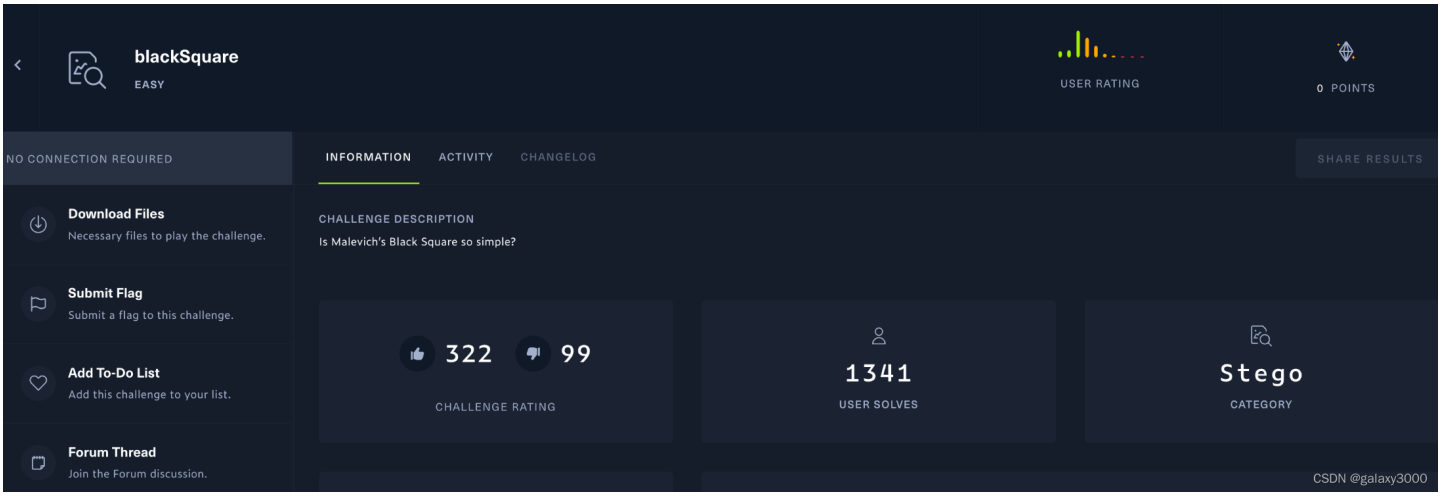
11 篇文章 0 订阅

订阅专栏

文章目录

概述

HackTheBox 网站CTF靶场杂项（Misc）相关题目blackSquare，题目地址https://app.hackthebox.com/challenges/blacksquare，主要考察图片隐写术和摩斯码的知识点。



解题

题目概述

下载附件得到blackSquare.zip，解压缩得到blackSquare.png

使用`file`查看文件类型，为png图片

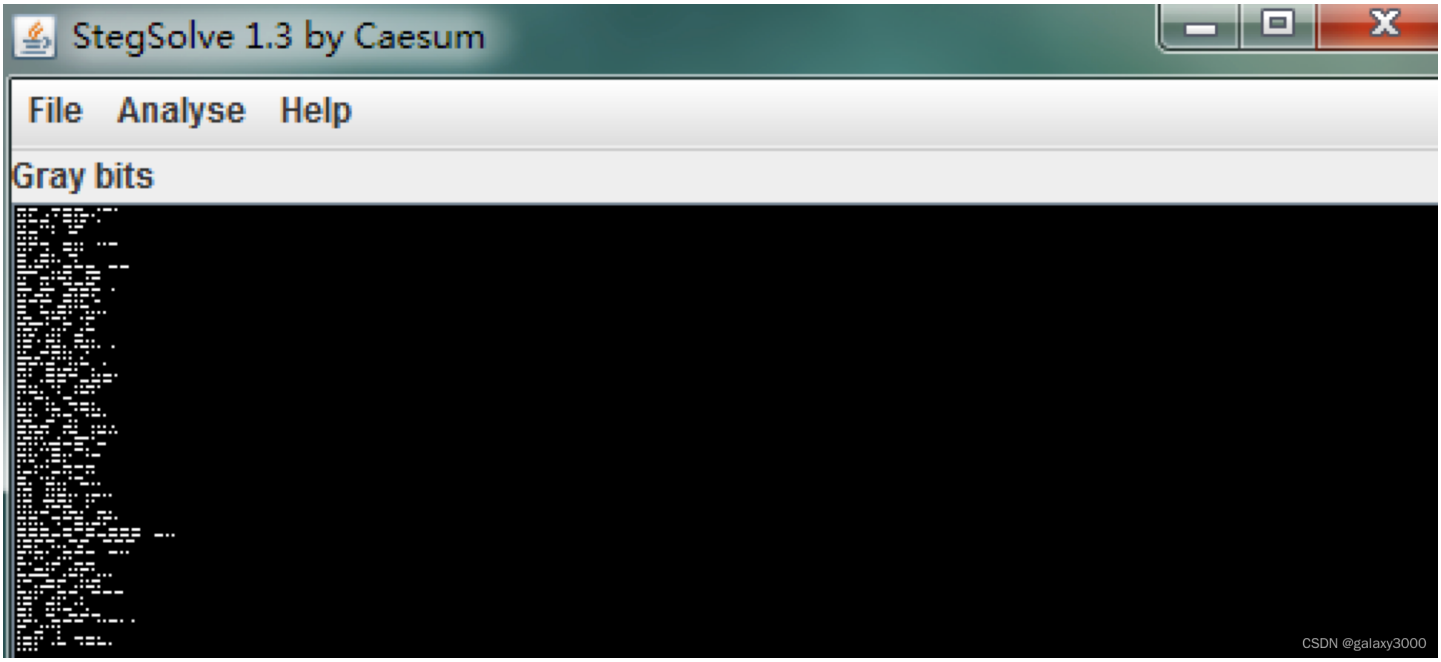
```
➜  Desktop file blackSquare.png
blackSquare.png: PNG image data, 500 x 500, 8-bit/color RGB, non-interlaced
```

解题过程

使用`exiftool`查看图片信息

```
➜  Desktop exiftool blackSquare.png
ExifTool Version Number         : 11.42
File Name                       : blackSquare.png
Directory                       : .
File Size                       : 252 kB
File Modification Date/Time     : 2020:01:13 08:32:48+08:00
File Access Date/Time           : 2022:02:20 07:26:38+08:00
File Inode Change Date/Time     : 2022:02:20 07:25:30+08:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 500
Image Height                    : 500
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 500x500
Megapixels                      : 0.250
```

使用StegSolve，在Grey bits中发现线索



放大查看

典型的摩斯码，对应的字母与符号如下

摩尔斯电码表

字符	电码符号	字符	电码符号	字符	电码符号
A	• —	N	— •	1	• — — — —
B	— • • •	O	— — —	2	• • — — —
C	— • — •	P	• — — •	3	• • • — —
D	— • •	Q	— — • —	4	• • • • —
E	•	R	• — •	5	• • • • •
F	• • — •	S	• • •	6	— • • • •
G	— — •	T	—	7	— — • • •
H	• • • •	U	• • —	8	— — — • •
I	• •	V	• • • —	9	— — — — •
J	• — — —	W	• — —	0	— — — — —
K	— • —	X	— • • —	?	• • — — • •
L	• — • •	Y	— • — —	/	— • • — •
M	— —	Z	— — • •	( )	— • — — • —
				—	— • • • • —
				•	• — — — —

编写python脚本

```
import re
import sys
import string
from PIL import Image

morseAlphabet = {"A": ".-","B": "-...","C": "-.-.","D": "-..","E": ".","F": "..-.","G": "--.","H": "....","I": "
..",
"J": ".---","K": "-.-","L": ".-..","M": "--","N": "-.","O": "---","P": ".--.","Q": "--.-","R": ".-.","S": "...",
"T": "-","U": "..-",V": "...-","W": ".--","X": "-..-","Y": "-.--","Z": "--..","  ": "/","1" : ".----","2" : "..--
-",
"3" : "...--","4" : "....-","5" : ".....","6" : "-....","7" : "--...","8" : "---..","9" : "----.","0" : "-----",
".": ".-.-.-",",": "--..--",":": "---...","?": "..--..","'": ".----.","-": "-....-","/": "-..-.","@": ".--.-.",
"=": "-...-"}

inverseMorseAlphabet = dict((v, k) for (k, v) in morseAlphabet.items())
def decodedMorse(message):
    msgSeparated = message.split(' ')
    decMessage = ''
    for char in msgSeparated:
        if char in inverseMorseAlphabet:
            decMessage += inverseMorseAlphabet[char]
        else:
            decMessage += '<CNF>'
    print ("decMessage= ", decMessage)
    return decMessage

image = Image.open("blackSquare-filterd.png")
rgb = image.convert("RGB")
width, height = image.size
myString = ""
for y in range(0, height, 1):
    myString += "\n"
    for x in range(0, width, 1):
        pixel = rgb.getpixel((x,y))
        myString += ("0","1")[pixel[0] == 255]

myString = (myString.replace("0001", "-"))
myString = (myString.replace("01", "."))
myString = re.sub('1+', ' ', myString)
myString = re.sub('\s+', ' ', myString)
myString = myString.strip()
print(myString)

decodedMorse(myString)
```

运行脚本即可得到包含flag的字符串。