HackTheBox-Hackerman

原创

galaxy3000 于 2022-02-20 07:16:04 发布 118 收藏

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

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

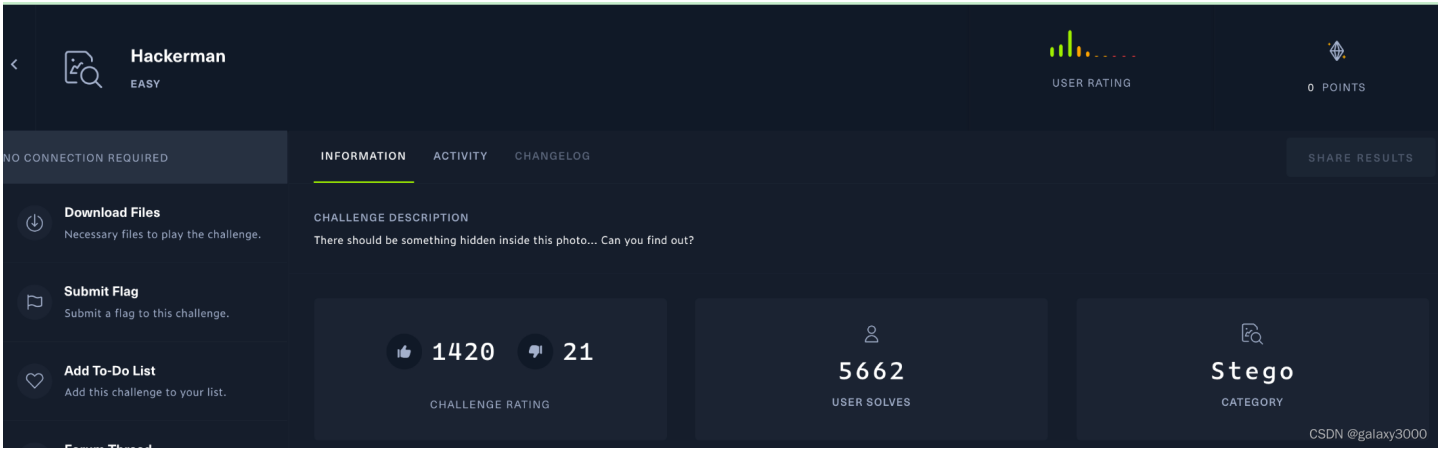
解题

题目概述

解题过程

概述

HackTheBox 网站CTF靶场杂项（Misc）相关题目Hackerman，题目地址https://app.hackthebox.com/challenges/hackerman，主要知识点为图片的隐写术。



解题

题目概述

下载附件Hackerman.zip，解压缩得到hackerman.jpg。

使用`file`查看文件类型，为jpg格式图片。

```
➜  Desktop file hackerman.jpg
hackerman.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, s
egment length 16, baseline, precision 8, 960x540, frames 3
```

解题过程

使用`exiftool`查看图片信息，未发现可利用的信息。

```
➜  Desktop exiftool hackerman.jpg
ExifTool Version Number         : 11.42
File Name                       : hackerman.jpg
Directory                       : .
File Size                       : 119 kB
File Modification Date/Time     : 2017:07:26 09:52:10+08:00
File Access Date/Time           : 2022:02:20 07:09:25+08:00
File Inode Change Date/Time     : 2022:02:20 07:08:39+08:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 960
Image Height                    : 540
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 960x540
Megapixels                      : 0.518
```


根据题目提示，**There should be something hidden inside this photo**，使用steghide提取图片中的隐藏文件，提示需要密码。

```
(pyenv3) ➜  tmp steghide extract -sf hackerman.jpg
Enter passphrase:
```

使用stegcracker破解密码，得到隐藏的文件

```
stegcracker hackerman.jpg rockyou.txt
```

```
(pyenv3) ➜  tmp stegcracker hackerman.jpg rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'hackerman.jpg' with wordlist 'rockyou.txt'..
Successfully cracked file with password: almost
Tried 11476 passwords
Your file has been written to: hackerman.jpg.out
almost
```


使用`file`查看文件类型，为文本文件

```
(pyenv3) ➜  tmp file hackerman.jpg.out
hackerman.jpg.out: ASCII text
```

查看此文件，得到base64编码的字符串

```
(pyenv3) ➜  tmp cat hackerman.jpg.out
SFRCezN2MWxfYzBycH0=
```

base64解码得到flag

```
(pyenv3) ➜  tmp cat hackerman.jpg.out | base64 -d
HTB{3v[redacted]p}%
```