

HackTheBox-Beatles

原创

galaxy3000 于 2022-02-22 09:19:55 发布 278 收藏

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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/galaxy3000/article/details/123060479>

版权

Misc

[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Beatles, 题目地址<https://app.hackthebox.com/challenges/beatles>, 主要考察图片隐写术、zip压缩包与rot13替换式密码等综合知识点。

The screenshot shows the HackTheBox challenge page for 'Beatles'. The challenge is categorized as 'EASY' and has a 'NO CONNECTION REQUIRED' status. The challenge description reads: 'John Lennon send a secret message to Paul McCartney about the next music tour of Beatles... Could you find the message and submit the flag?'. The challenge has a rating of 1065 and 142 user solves. The category is 'Stego'. The page also shows a 'Download Files' section with necessary files for the challenge and a 'Submit Flag' section. The user's profile 'galaxy3000' is visible in the bottom right corner.

解题

题目概述

下载附件Beatles.zip，解压缩得到如下文件。

名称	修改日期	大小	种类
BAND.zip	2017年9月24日 14:16	57 KB	ZIP 归档
m3ss@g#_f0r_pAuL	2017年9月24日 14:18	263 字节	Hex Fie...p 文稿

解题过程

查看文件m3ss@g#_f0r_pAuL

Ur1 Cnhy,

Zl Sbyqre unf cnffcuenfr jvgu sbhe (4) punenpgref.

Pbhyq lbh spenpx vg sbe zr???

V fraq lbh n zrffntr sbe bhe Gbhe arkg zbagu...

Qba'g Funer vg jvgu bgure zrzuref bs bhe onaq...

-Wbua Yraaba

CF: Crnpr naq Ybir zl sevraq... Orngyrf Onaq sbe rire!

看着像是一段话，但意思不可识别，尝试rot13，得到可识别的文字

Recipe

ROT13

Rotate lower case chars Rotate upper case chars Rotate numbers

Amount: 13

Input

Ur1 Cnhy,
Zl Sbyqre unf cnffcuenfr jvgu sbhe (4) punenpgref.
Pbhyl lbh spenpx vg sbe zr???
V fraq lbh n zrffntr sbe bhe Gbhe arkg zbagu...
Qba'g Funer vg jvgu bgure zrzuref bs bhe onaq...
-Wbua Yraaba
CF: Crnpr naq Ybir zl sevraq... Orngyrf Onaq sbe rire!

Output

Hey Paul,
My Folder has passphrase with four (4) characters.
Could you fcrack it for me???
I send you a message for our Tour next month...
Don't Share it with other members of our band...
-John Lennon
PS: Peace and Love my friend... Beatles Band for ever!

核心意思是说密码由4个字符组成。

使用fcrackzip构造4位字符密码破解zip压缩包。

```
fcrackzip -b -c 'a' -l 4 -u BAND.zip
```

```
→ tmp fcrackzip -b -c 'a' -l 4 -u BAND.zip
```

```
PASSWORD FOUND!!!!: pw == pass
```

THE BEATLES



CSDN @galaxy3000

使用steghide提取，使用密码 `pass` 无效，使用图片文字 `THEBEATLES` 成功

```
→ tmp steghide extract -sf BAND.JPG
Enter passphrase:
wrote extracted data to "testabeattle.out".
```

使用 `file` 查看文件类型，为elf文件

```
→ tmp file testabeattle.out
testabeattle.out: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=ca68ea305ff7d393662ef8ce4e5eed0b478c8b4e, not stripped
```

使用逆向框架radare2查看文件中的字符串

```
→ tmp r2 testabeatle.out
[0x000005a0]> iz
[Strings]
nth paddr      vaddr      len size section type  string
-----
0  0x00000878 0x00000878 62 63  .rodata ascii Hey Paul! If you are here... Give my your favourite character!
1  0x000008c0 0x000008c0 105 106 .rodata ascii Ok Paul... A little challenge for you mate, cause last month som
eone crazy man hacked...WTF! Let's Begin!
2  0x00000930 0x00000930 109 110 .rodata ascii #####Challenge#####
#####
3  0x000009a0 0x000009a0 33 34  .rodata ascii Tell me PAul! The result of 5+5?
4  0x000009c8 0x000009c8 64 65  .rodata ascii Ok!ok! it was easy... Tell me now... The result of: 5+5-5*(5/5)?
5  0x00000a10 0x00000a10 73 74  .rodata ascii Last one! The result of: (2.5*16.8+1.25*10.2+40*0.65+1.5*7.5+1.2
5*3.2):40
6  0x00000a60 0x00000a60 38 39  .rodata ascii Hey Paul! nice!!! this is the message
7  0x00000a88 0x00000a88 180 181 .rodata ascii VGhlIHRvdXIgd2FzIGNhbmNlbGVkIGZvciB0aGUgZm9sbG93aW5nIG1vbnRoLi4u
IQ0KQDQpJJ2xsIGdvIG91dCBmb3IgzG1ubmVYIHdpdGggbXkgZ2lybGZyaWVuZCBuYW1lZCBZb2NvISA7KQ0KDQpIVEJ7UzByUnlftXlfRlIxM25EfQ0K
Q0K
8  0x00000b40 0x00000b40 105 106 .rodata ascii WTF! You are not Paul!! SOS SOS SOS HACKER HERE!! I will call th
e police someone want to steal my data!!!
9  0x00000bb0 0x00000bb0 116 117 .rodata ascii #####END OF CHALLENGE#####
#####
CSDN @galaxy3000
```

得到

```
VGhlIHRvdXIgd2FzIGNhbmNlbGVkIGZvciB0aGUgZm9sbG93aW5nIG1vbnRoLi4uIQ0KQDQpJJ2xsIGdvIG91dCBmb3IgzG1ubmVYIHdpdGggbXkgZ2lybGZyaWVuZCBuYW1lZCBZb2NvISA7KQ0KDQpIVEJ7UzByUnlftXlfRlIxM25EfQ0K
```

base64解码得到flag

```
→ tmp rax2 -D 'VGhlIHRvdXIgd2FzIGNhbmNlbGVkIGZvciB0aGUgZm9sbG93aW5nIG1vbnRoLi4uIQ0KQDQpJJ2xsIGdvIG91dCBmb3IgzG1ubmVYIHdpdGggbXkgZ2lybGZyaWVuZCBuYW1lZCBZb2NvISA7KQ0KDQpIVEJ7UzByUnlftXlfRlIxM25EfQ0K'
The tour was canceled for the following month...!

I'll go out for dinner with my girlfriend named Yoco! ;)

HTB{S[REDACTED]D}
```

CSDN @galaxy3000