

攻防世界 Misc高手进阶区 3分题 flag_universe

原创

思源湖的鱼 于 2020-11-09 10:35:37 发布 1538 收藏

分类专栏: [ctf](#) 文章标签: [网络安全](#) [ctf](#) [攻防世界](#) [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/weixin_44604541/article/details/109570910

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

本篇是flag_universe的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个流量包

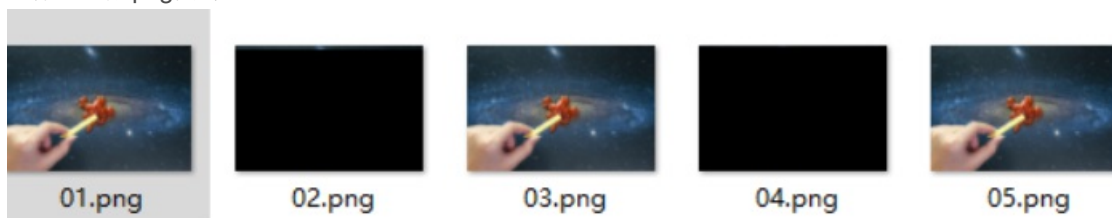
扔进wireshark

追踪tcp流, 发现是FTP传输文件, 传输的是一张图片

```
90 Response: 226 Directory send OK.  
72 Request: PASV  
114 Response: 227 Entering Passive Mode (172  
86 Request: RETR /universe.png  
142 Response: 150 Opening BINARY mode data c  
90 Response: 226 Transfer complete.  
72 Request: PASV  
114 Response: 227 Entering Passive Mode (172
```

在3、4、6、11、13、14处发现png图片的数据流以及7、8处的base64加密的假的flag值

仔细观察发现4和11处的数据不完整，缺少png尾部
其余用winhex进行处理成png图片



然后扔进stegsolve

无果

扔进zsteg

```
zsteg 1.png
.. text: "\n\n\n111???"
.. text: "E26*rg_90z"
.. text: "flag{Plate_err_klaus_Mail_Life}\n"
.. file: PGP Secret Sub-key -
.. text: "zC`XUWS"
```

得到flag

结语

知识点

- 流量追踪
- lsb隐写