攻防世界 Misc高手进阶区 2分题 心仪的公司

原创

思源湖的鱼 于 2020-11-02 16:36:08 发布 858 收藏 1

分类专栏： ctf 文章标签： 攻防世界 ctf misc wireshark

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109451538

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2分题

本篇是心仪的公司的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

搜索关键词

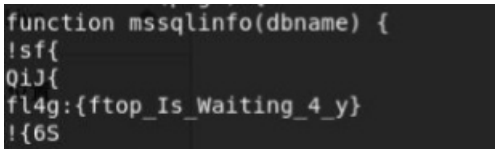
无果

追踪流量

看花眼

用linux的strings

```
strings webshell.pcapng | grep {
strings webshell.pcapng | grep -E0 '^....*?{....*?}$' 也可以用这个
```



得到flag

回头再在wireshark里翻

```
s@.(.N`k.UuUI.D.......o.....c...i.H.m..j...x....t....
?.].b......9.;.....n5...f]$.6..r....0.b.......D,.*.WMa.B.....+a<....bh.............&..<.~8.hgvq;.N..w.....q;.N.v...L.;.
6i.*.N..Ls.....q;.N.......i....c...fl4g:{ftop_Is_Waiting_4_y}
```

也能找到

结语

简单的strings命令