

攻防世界-MISC: embarrass

原创

LY613313 于 2021-11-26 15:18:41 发布 157 收藏

文章标签: 安全

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/m0_56161093/article/details/121559955

版权

这是攻防世界高手进阶区的第二题, 题目如下:

embarrass 43 最佳Writeup由随便娶一个 · jerrita提供

难度系数: ★ 1.0

题目来源: ciscn-2017

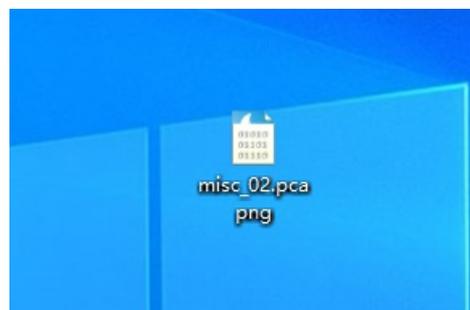
题目描述: 暂无

题目场景: 暂无

题目附件: 附件1

CSDN @LY313613

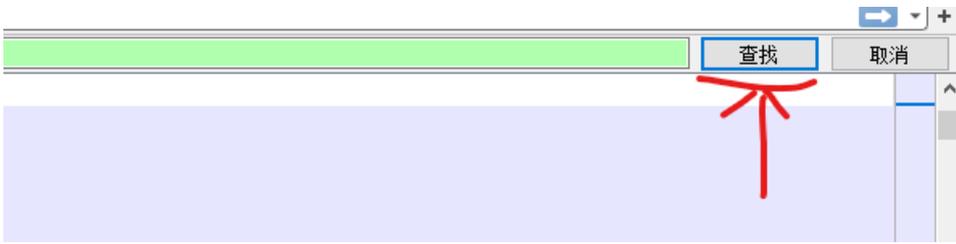
点击下载附件一, 得到一个压缩包, 解压后得到一个流量包



用wireshake打开, CTRL+F搜索字符串flag, 记住要选择分组字节流

Time	Source	Destination	Protocol	Length	Info
2756	182.211661	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4496161 Win=262144 Len=0
2757	182.211661	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4499437 Win=262144 Len=0
2758	182.212815	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4503105 Win=262144 Len=0
2759	182.213379	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4506577 Win=262144 Len=0
2760	182.213952	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4510049 Win=262144 Len=0
2761	182.214539	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4513521 Win=262144 Len=0
2762	182.214540	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4514037 Win=261624 Len=0
2763	182.215143	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4516993 Win=262144 Len=0
2764	182.215689	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4520465 Win=262144 Len=0
2765	182.216267	192.168.197.1	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=4521985 Win=262144 Len=0
2766	182.216449	192.168.197.128	FTP-DA...	32822	FTP Data: 32768 bytes (PASV) (SIZE misc2.pcapng)

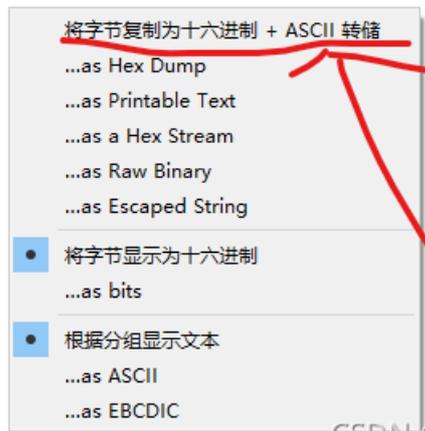
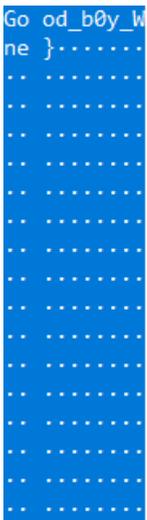
点击查找



在点击几次过后即可看到flag（我记我是点了6次）

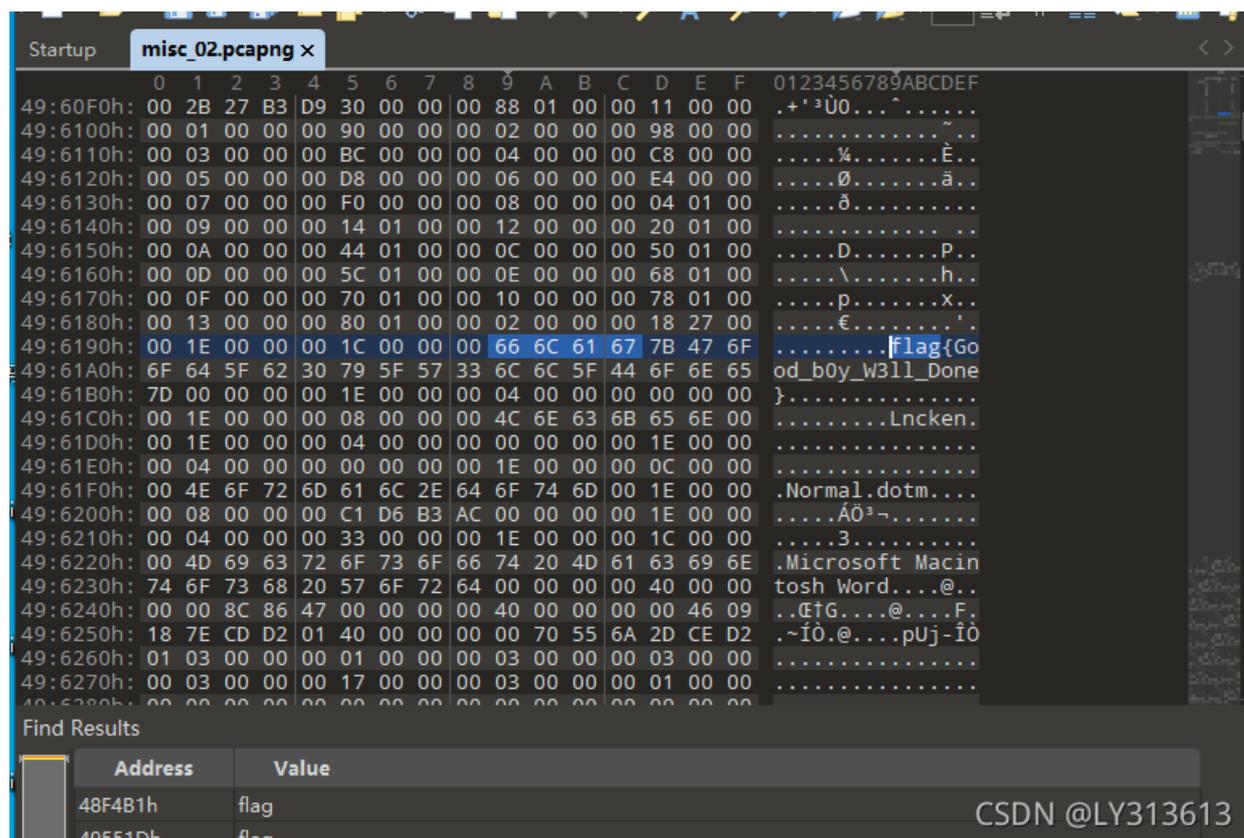
```
[Time since first frame in this TCP stream: 0.724521000 seconds]
[Time since previous frame in this TCP stream: 0.000182000 seconds]
P payload (32768 bytes)
Data (32768 bytes data)
ip_frame: 1236]
in_method: PASV1
30 66 6c 61 67 7b 47 6f 6f 64 5f 62 30 79 5f 57  -flag{Go od_b0y_W
33 6c 6c 5f 44 6f 6e 65 7d 00 0c 10 00 00 02 00  311_Done }.....
30 00 1e 00 00 00 05 00 00 00 b1 ea cc e2 00 03  .....
30 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00  .....
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..CSDN @LY313613
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

复制提交成功，如果复制不了，可以先右键，选择将字节复制为16进制+ASCII转储，将其复制到文本文档里面再查找复制。



```
flag{Good_b0y_W311_Done}
```

提交过后查看一下WP发现其实用16进制编辑器打开直接查找即可，用010editor打开查找flag，直接就可以得到flag（学到了□□□□）



以上就是我对这道题的解法。因本人菜鸡一只，如果有什么不对的地方，实属正常。还请各位大佬予以指正，谢谢！