




【愚公系列】2021年11月 攻防世界-进阶题-MISC-002(embarrass)

原创

愚公搬代码  于 2021-10-29 10:26:06 发布  21407  收藏

分类专栏: [#CTF-攻防世界-MISC](#) 文章标签: [网络安全](#) [系统安全](#) [web安全](#) [安全架构](#) [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/aa2528877987/article/details/121029459>

版权



[CTF-攻防世界-MISC 专栏收录该内容](#)

98 篇文章 0 订阅

订阅专栏

文章目录

[一、embarrass](#)

[二、答题步骤](#)

[1.搜索字符串](#)

[总结](#)

一、embarrass

文件: 攻防世界下载对应文件

二、答题步骤

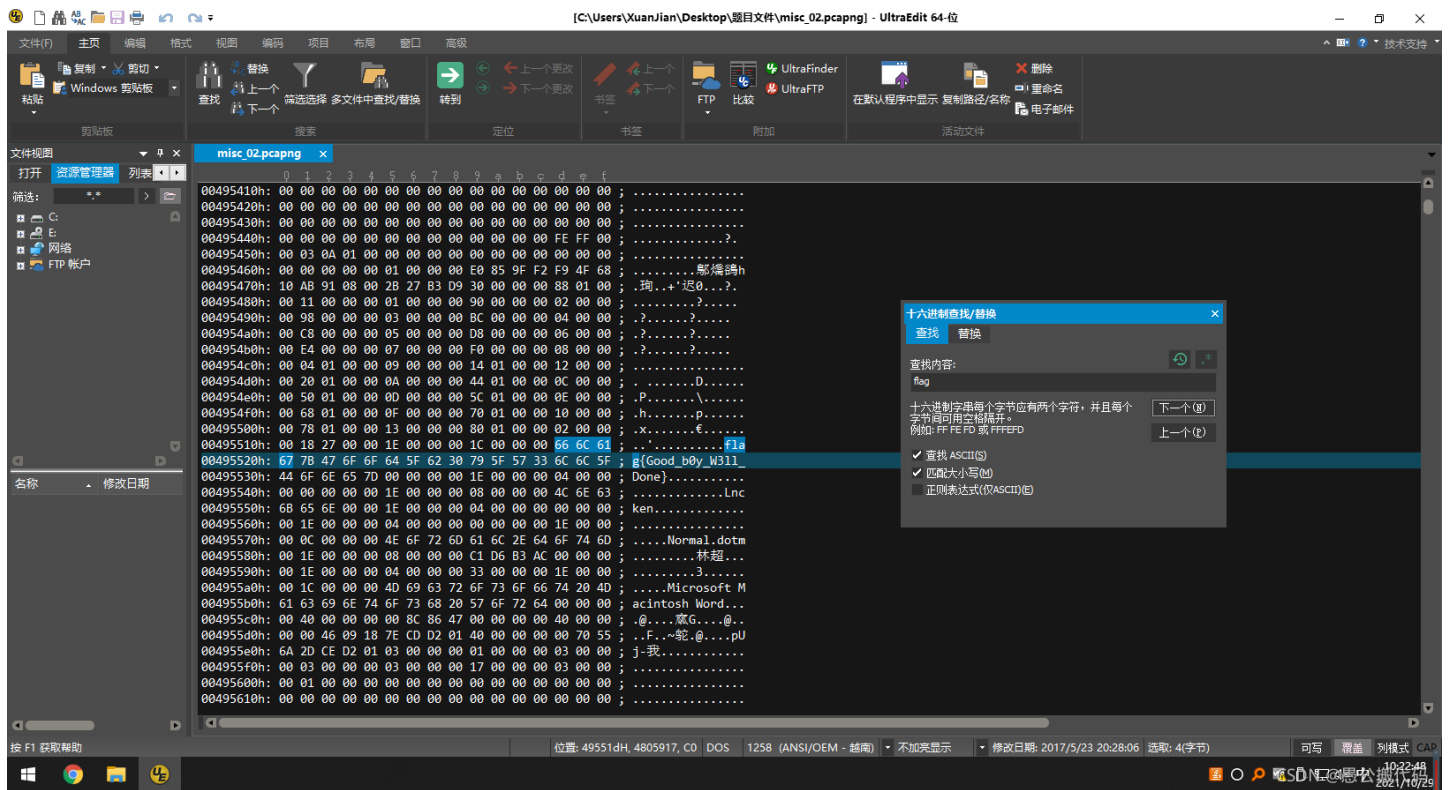
1.搜索字符串

解法一: Wireshark搜索字符串

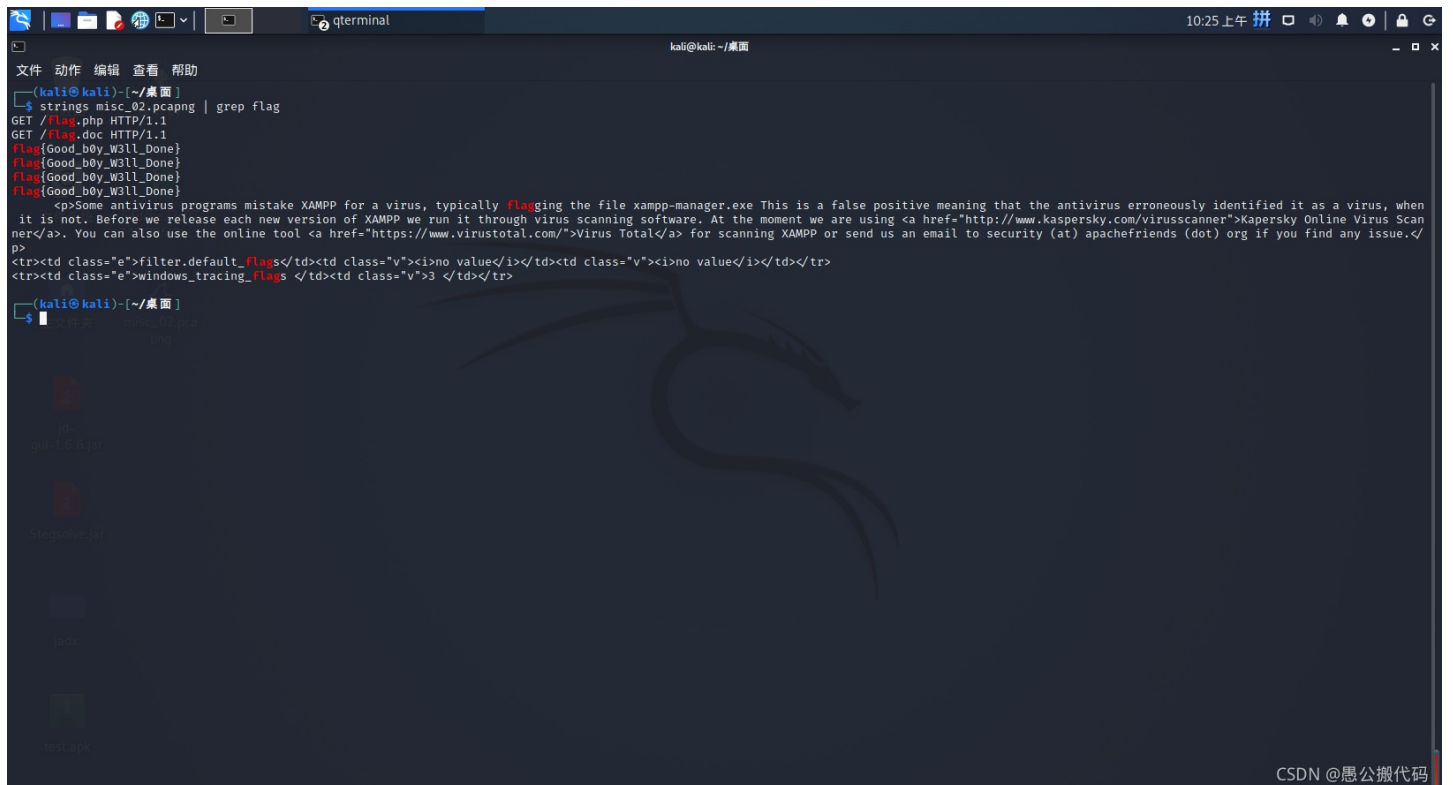
The screenshot shows the Wireshark interface with the following details:

- Packet List:** A table of captured packets. Packet 2766 is selected, showing it is an FTP-DA packet of length 32822 bytes, containing FTP Data.
- Packet Details:**
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 32808
 - Identification: 0x1dc6 (7622)
 - Flags: 0x4000, Don't fragment
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.197.128
 - Destination: 192.168.197.1
 - Transmission Control Protocol, Src Port: 52176, Dst Port: 3360, Seq: 4554753, Ack: 1, Len: 32768
 - FTP Data (32768 bytes data)
- Packet Bytes:** A hex dump of the selected packet's data. The string "flag(Go od_b0y_kill_Done)" is visible in the ASCII column.

解法二：十六进制工具搜索字符串



解法三：linux下 strings misc_02.pcapng | grep flag



总结

- Wireshark
- strings
- winhex