

# xctf Cephalopod

原创

fa1c4 于 2020-11-29 11:17:33 发布 304 收藏

分类专栏: [MISC](#) 文章标签: [信息安全](#)

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/qq\\_33976344/article/details/110307013](https://blog.csdn.net/qq_33976344/article/details/110307013)

版权



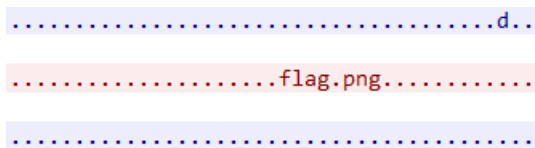
[MISC 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

## Cephalopod

一个流量包, 追踪TCP流发现flag.png字样, 想办法提取出来



到kali下,binwalk和foremost打一套

发现提取不了flag.png文件

尝试xtract提取

安装

```
sudo apt-get install tcpextract
```

提取

```
tcpextract -f cepha.pcap
```

结果

```
falca@kali-297:~/Desktop$ tcpextract -f cepha.pcap  
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], ex  
porting to 00000000.png  
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], ex  
porting to 00000001.png
```

发现在linux下打开有问题, 换到win下打开



HITB{95700d8aefdc1648b90a92f3a8460a2c}

最后提取图中文字得到flag



HITB{95700d8aefdc1648b90a92f3a8460a2c}