De1ctf 2020 -'Misc杂烩' writeup

原创

尸者狗 于 2020-05-06 18:30:06 发布 580 收藏

分类专栏： ctf-writeup 文章标签： 安全

一道很有意思的流量分析+NTFS隐写

文章目录

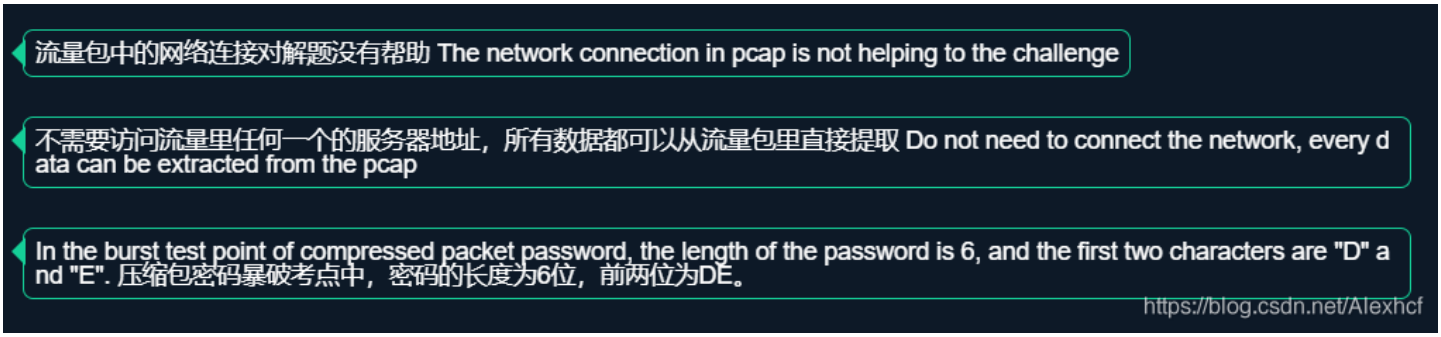
描述
文件地址
hint
writeup

描述

文件地址

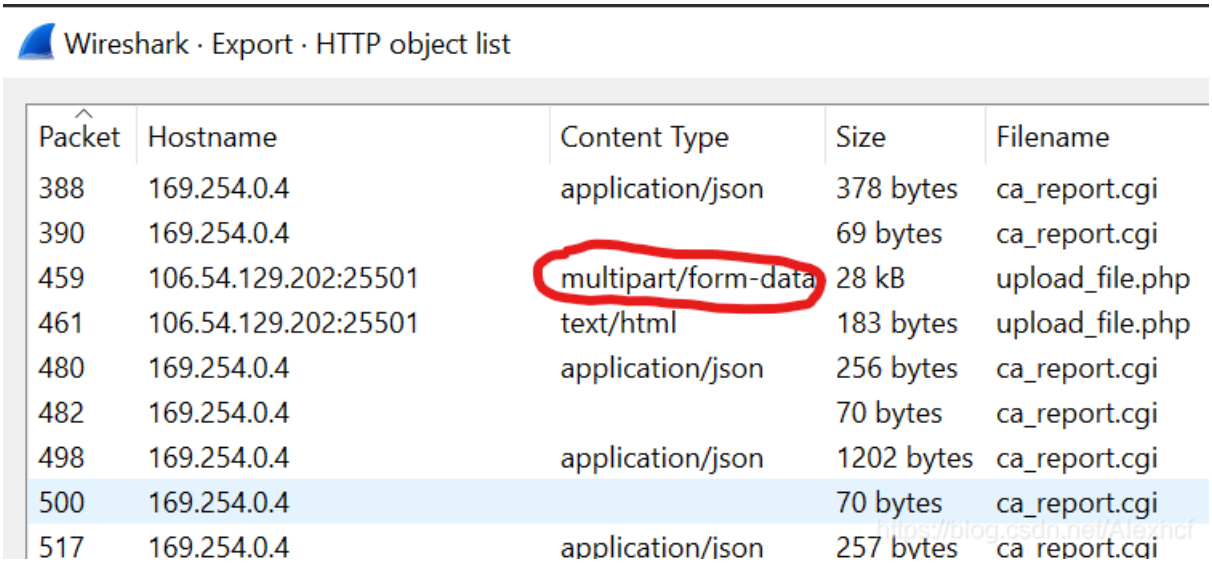
```
https://drive.google.com/file/d/1-SrQ8JbD8zAQNVlvuwu3T2Lbu_o1knRQ/view?usp=sharing
```

hint



writeup

下载文件，wireshark打开，看了下有很多post请求，文件-导出对象-http



然后会导出一堆文件，发现有几个名称为upload形式的，猜测应该就是他们

```
foremost upload_file*
```

输出有个png文件


```
https://drive.google.com/file/d/1JBdPj7eRaXuLCTFGn7AluAxmxQ4k1jvX/view
```

下载下来，binwalk几次得到一个压缩包

ARCHPR破解，根据hint设置掩码`DE????`,选择掩码攻击，得到DE34Q1，解压

得到一张照片，binwalk，得到一个txt`De1CTF{jaivy say that you almost get me!!! }`，明显是错的，这里用到的是ntfs隐写，

7z解压刚才binwalk分离出来的rar文件，打开能直接看到ntfs隐写的文件，找到flag在666.jpg_fffffffllll.txt；另外也可以用Sysinternals的Streams

获取流名称，然后使用Get-Content显示流的内容

下载刚才那个软件，把刚才kali里binwalk出来的东西都丢到有压缩密码的解压后文件夹，注意streams64.exe的位置`.\streams64.exe -s`，确认一下。


```
Get-Content -Path .\66DB\666.jpg -Stream ffffffffllllll.txt
```

真flag到手

```
PS C:\...\You_found_me_Orz> Get-Content -Path .\66DB\666.jpg -Stream ffffffffllllll.txt
"De1CTF{E4Sy_M1sc_By_Jaivy_31b229908cb9bb}"
```