

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](#)

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/Alexhcf/article/details/105952647>

版权



[ctf-writeup](#) 专栏收录该内容

6 篇文章 1 订阅

订阅专栏

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-SrQ8JbD8zAQNV1vuwu3T2Lbu_o1knRQ/view?usp=sharing

hint

流量包中的网络连接对解题没有帮助 The network connection in pcap is not helping to the challenge

不需要访问流量里任何一个的服务器地址, 所有数据都可以从流量包里直接提取 Do not need to connect the network, every data can be extracted from the pcap

In the burst test point of compressed packet password, the length of the password is 6, and the first two characters are "D" and "E". 压缩包密码爆破考点中, 密码的长度为6位, 前两位为DE。

<https://blog.csdn.net/Alexhcf>

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

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
388	169.254.0.4	application/json	378 bytes	ca_report.cgi
390	169.254.0.4		69 bytes	ca_report.cgi
459	106.54.129.202:25501	multipart/form-data	28 kB	upload_file.php
461	106.54.129.202:25501	text/html	183 bytes	upload_file.php
480	169.254.0.4	application/json	256 bytes	ca_report.cgi
482	169.254.0.4		70 bytes	ca_report.cgi
498	169.254.0.4	application/json	1202 bytes	ca_report.cgi
500	169.254.0.4		70 bytes	ca_report.cgi
517	169.254.0.4	application/ison	257 bytes	ca_report.cgi

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>

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

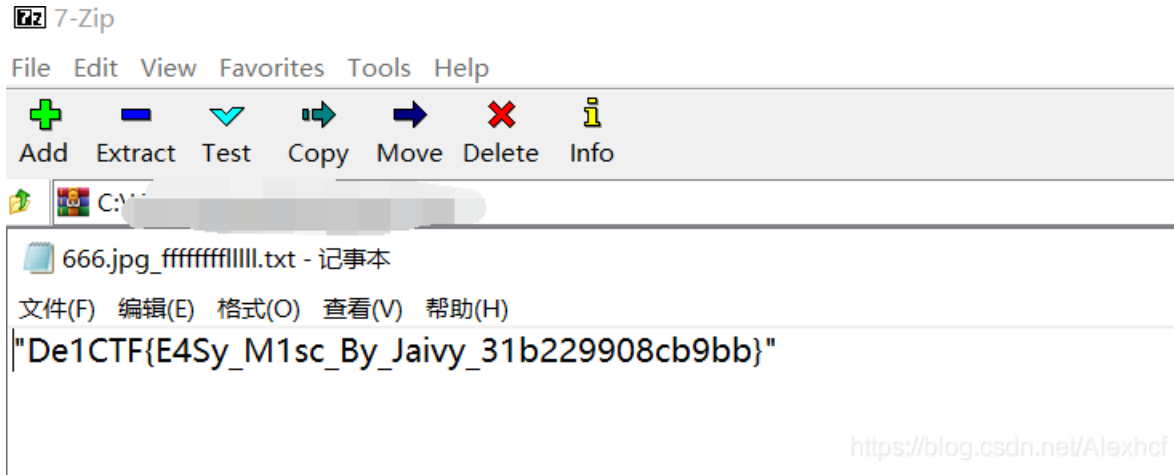
下载下来，binwalk几次得到一个压缩包

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

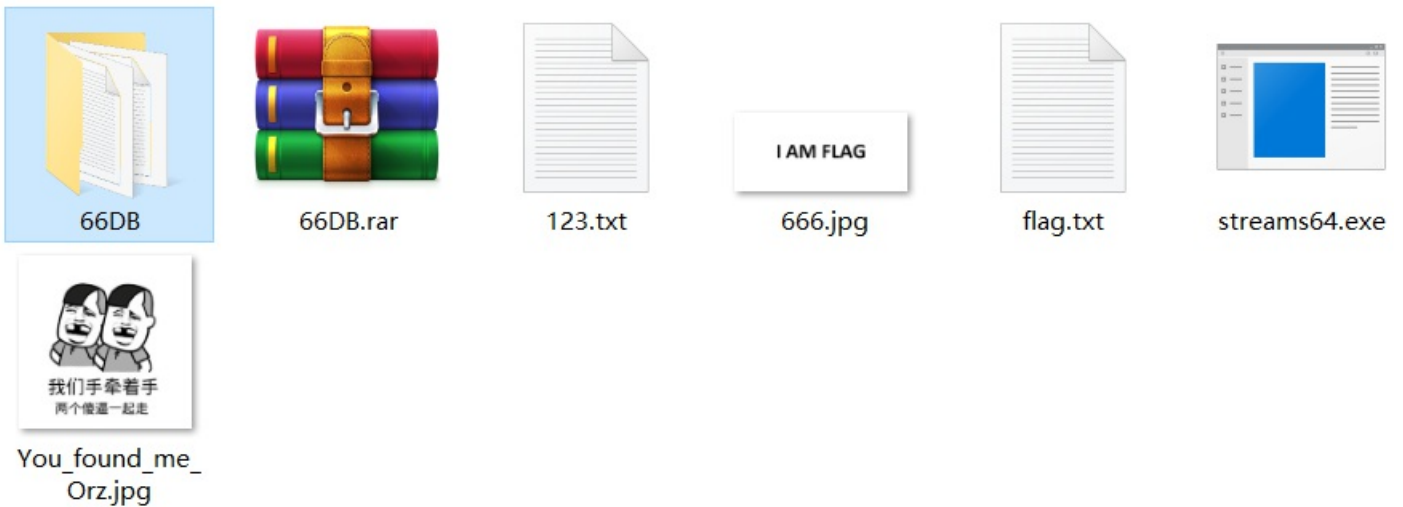
得到一张照片，binwalk，得到一个txt De1CTF{jaivy say that you almost get me!!! }，明显是错的，这里用到的是ntfs隐写，

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_ffffffl1111.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 ffffffffl1111.txt
```

真flag到手

```
PS C:\...> Get-Content -Path .\66DB\666.jpg -Stream ffffffffl1111.txt  
"De1CTF{E4Sy_M1sc_By_Jaivy_31b229908cb9bb}"
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)