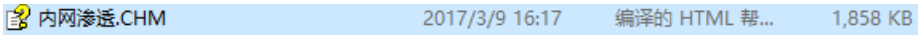
一道关于chm设计ctf钓鱼的一些思考

转载

weixin_30820077 于 2017-06-09 10:14:00 发布 63 收藏
原文链接：http://www.cnblogs.com/adislj777/p/6970637.html

题目：flag就是文件指向的地址

文件：

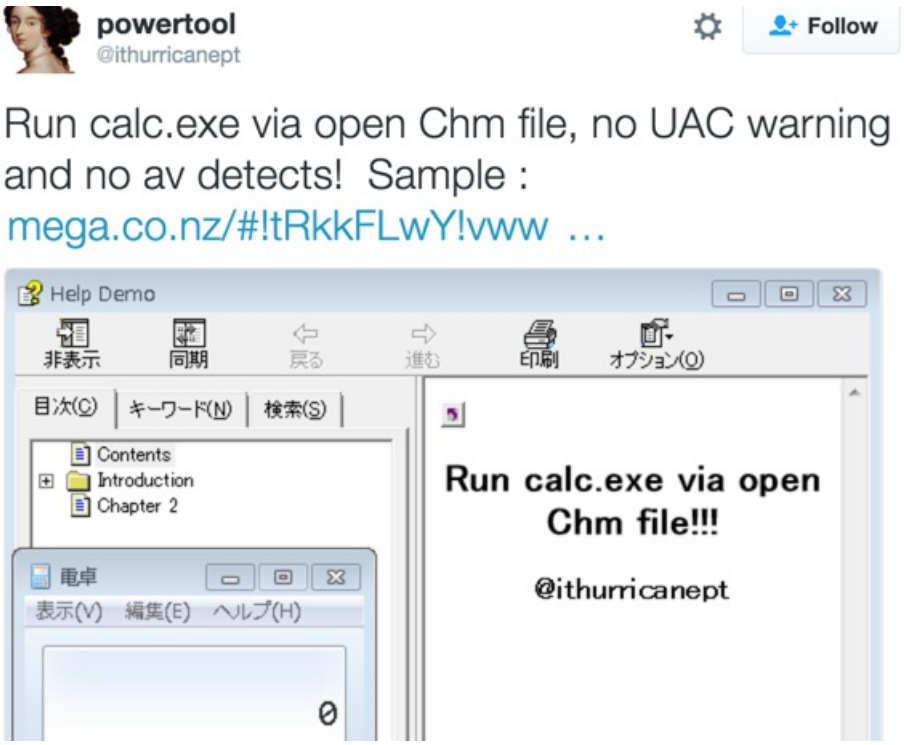


作为一名web狗的出题人，这道ctf有点意思不是在于因为它难，而是相对于一些代码审计以及一些杂项题来说，它只是很好玩。

首先，我们看到题目是一个chm文件。chm文件在钓鱼中比较常见的。比如很久以前的那些动作片种子，下载回来总会有个chm文件的图片简介在文件目录下，那些充满诱惑的FBI warning，以及当你点击xxxavi.chm的时候。

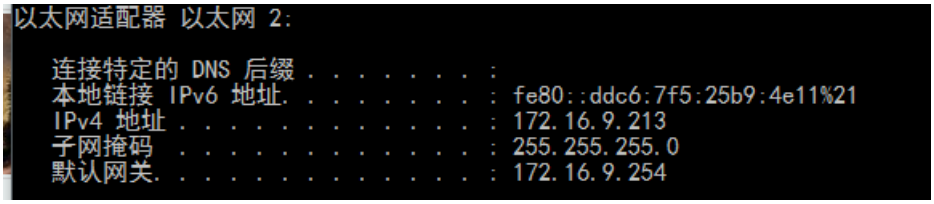
相对于pdf绑马以及之前比较新Word漏洞CVE-2017-0199。它是我所知在win下伪装的比较好的一个。可以参考ping：CHM渗透：从入门到“入狱”

writeup普及：CHM（Compiled Help Manual）即“已编译的帮助文件”。它是微软新一代的帮助文件格式，利用HTML作源文，把帮助内容以类似数据库的形式编译储存。CHM支持Javas cript、VBs cript、ActiveX、Java Applet、Flash、
常见图形文件(GIF、JPEG、PNG)、音频视频文件(MID、WAV、AVI)等等，并可以通过URL与Internet联系在一起。因为使用方便，形式多样也被采用作为电子书的格式。以及下图



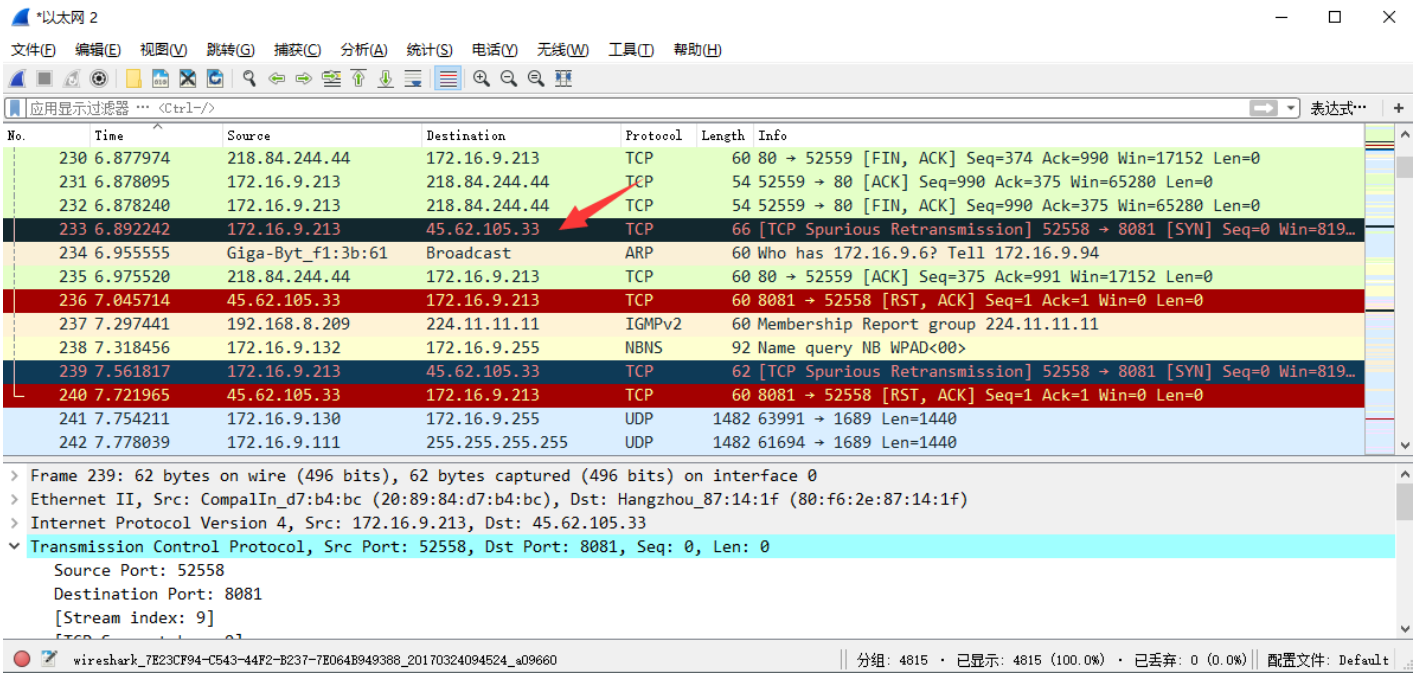
 No UAC and No AV 的EXEC

根据这些知识，以及题目所问的，找出文件指向的地址即是后门连接的服务器就是flag。根据后门连接一般采用TCP或者DNS。这里根据自己pc的ip。

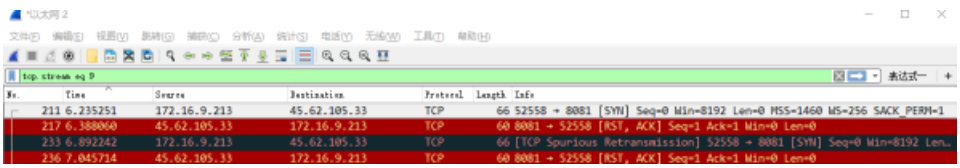


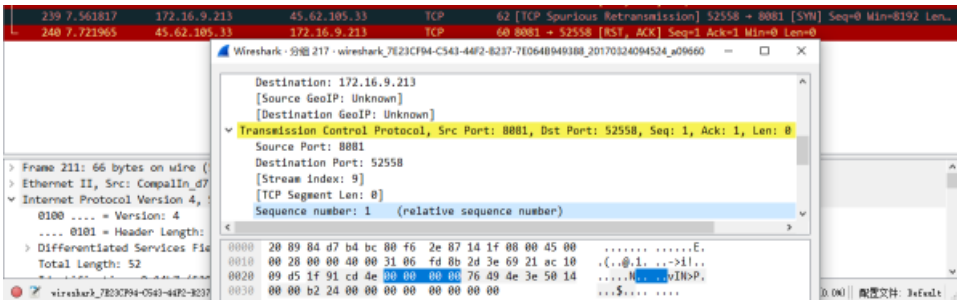
筛选tcp或者dns过滤大部分流量出来
ip.addr == 172.16.9.213 and tcp
以及一些标志符：

SYN表示建立连接，
FIN表示关闭连接，
ACK表示响应，
PSH表示有 DATA数据传输，
RST表示连接重置。

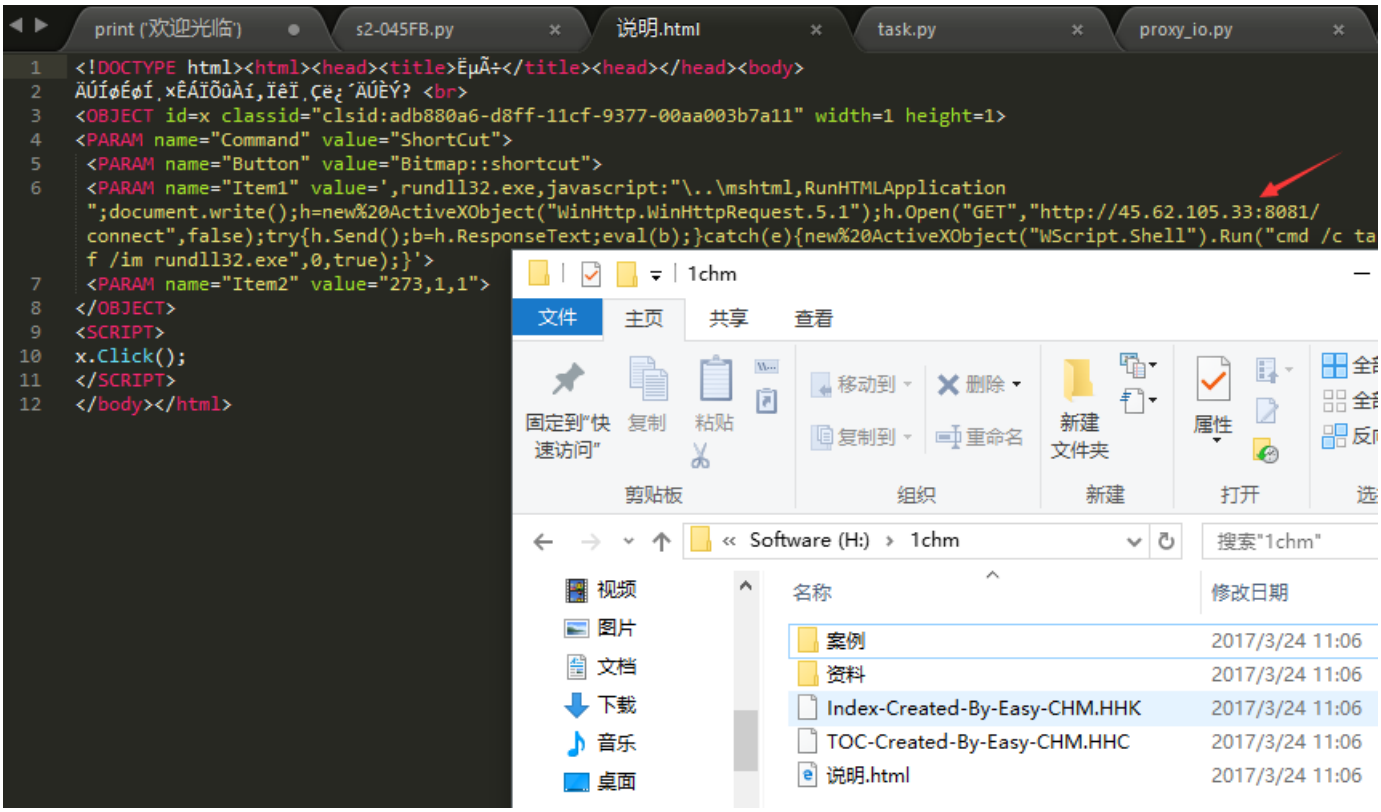


可以发现xxx.xxx.xxx.xxx在与本机进行tcp的通信，根据两个tcp的两个标识RST ack。可以发现文件在与服务器进行通信。这里flow下这些tcp流，确定文件指向的后门服务器地址。
这里cobalt strike 的teamserver没有开启，但是可以确定在双方在“串通”进行尝试握手。

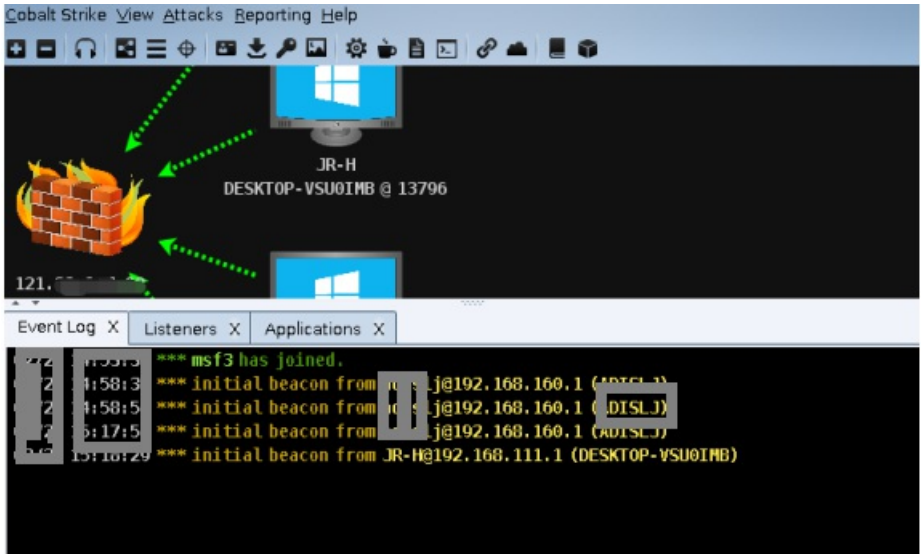




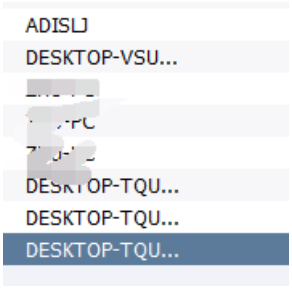
另一种方法溯源 chm是可以反编译为html的。 使用windows自带的hh.exe 则可进行反编译。hh -decompile h:\1chmF:\1.chm 【1.chm是内网渗透.chm，这里改了一下名字】



很典型的利用了chm exec 调用js，能做到免杀市面上很多杀毒软件，这里随便用了个测试截图



这里记录一次被黑与反杀的一个过程。



限号第一次发在土司上了。好久都没写博客，只好把笔记带上

分享一个我制作的免杀样本 链接：http://pan.baidu.com/s/1jH6mid4 密码：2qpa

一只在安全道路上慢跑的菜鸡

转载于:https://www.cnblogs.com/adislj777/p/6970637.html