

# 【CTF MISC】隐写术wireshark找出图片-“强网杯”网络安全挑战赛writeup

转载

[weixin\\_30782331](#) 于 2016-12-11 00:49:00 发布 1001 收藏

原文链接: <http://www.cnblogs.com/17bdw/p/6158828.html>

版权

这场CTF中有一道题是分析pcap包的。。

13.大黑阔:

从给的pcap包里把图片提取出来,是一张中国地图。

题目提示是黑阔在聊天,从数据里可以找出几段话。

思路:主要考察wireshark的过滤规则与熟悉度。

如果熟悉发送数据包的格式截取特定的字符串 "[{" ,就能找出聊天记录了,也可以通过以下两个步骤找出关键的图片。

1、通过http过滤语句过滤出聊天内容

```
((http) && !(frame.len == 78)) && !(frame.len == 312)
```

2、将数据包中的图片提取出来。

```
HTTP数据 - 查看POST数据包 - Media Type - 导出分组字节流
```

就可以将图片直接导出来了,如果用Winhex要从FFD8, FFD9头尾进行截取,则比较麻烦。

流量包.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
14056	478.027908	192.168.169.130	192.168.40.42	HTTP	1198	POST /upfile/upload_file.php HTTP/1.1 (image/jpeg)
2955	389.117807	192.168.40.42	192.168.169.130	HTTP	584	HTTP/1.1 200 OK (text/html)
551	74.207226	192.168.40.42	192.168.169.130	HTTP	375	HTTP/1.1 200 OK (text/html)
1973	262.471687	192.168.40.42	192.168.169.130	HTTP	374	HTTP/1.1 200 OK (text/html)
1552	207.364170	192.168.40.42	192.168.169.130	HTTP	369	HTTP/1.1 200 OK (text/html)
1213	161.348317	192.168.40.42	192.168.169.130	HTTP	369	HTTP/1.1 200 OK (text/html)
2436	320.100628	192.168.40.42	192.168.169.130	HTTP	367	HTTP/1.1 200 OK (text/html)
2557	336.097983	192.168.40.42	192.168.169.130	HTTP	366	HTTP/1.1 200 OK (text/html)
801	109.222696	192.168.40.42	192.168.169.130	HTTP	361	HTTP/1.1 200 OK (text/html)
964	129.297415	192.168.40.42	192.168.169.130	HTTP	360	HTTP/1.1 200 OK (text/html)
1461	194.347858	192.168.40.42	192.168.169.130	HTTP	358	HTTP/1.1 200 OK (text/html)
2657	350.097728	192.168.40.42	192.168.169.130	HTTP	355	HTTP/1.1 200 OK (text/html)
3443	453.441555	192.168.40.42	192.168.169.130	HTTP	353	HTTP/1.1 200 OK (text/html)
389	51.222191	192.168.40.42	192.168.169.130	HTTP	350	HTTP/1.1 200 OK (text/html)
1836	244.463764	192.168.40.42	192.168.169.130	HTTP	348	HTTP/1.1 200 OK (text/html)
1140	151.347703	192.168.40.42	192.168.169.130	HTTP	348	HTTP/1.1 200 OK (text/html)
14222	499.473229	192.168.40.42	192.168.169.130	HTTP	347	HTTP/1.1 200 OK (text/html)
2685	354.087073	192.168.40.42	192.168.169.130	HTTP	347	HTTP/1.1 200 OK (text/html)
1732	231.468320	192.168.40.42	192.168.169.130	HTTP	346	HTTP/1.1 200 OK (text/html)

[Full request URI: http://192.168.40.42/upfile/upload\_file.php]

[HTTP request 69/85]

[Prev request in frame: http://192.168.40.42/upfile/upload\_file.php]

[Response in frame: http://192.168.40.42/upfile/upload\_file.php]

[Next request in frame: http://192.168.40.42/upfile/upload\_file.php]

File Data: 7116180 bytes

MIME Multipart Media Encapsulation

[Type: multipart/form-data, Boundary: "-----7df3eb40102"]

First boundary: -----7df3eb40102

Encapsulated multipart part

Content-Disposition: form-data; name="file"; filename="map.jpg"

Content-Type: image/jpeg

Media Type

boundary: -----7df3eb40102\r\n

Encapsulated multipart part:

Last boundary: \r\n-----7df3eb40102--\r\n

转载于:<https://www.cnblogs.com/17bdw/p/6158828.html>



创作打卡挑战赛  
赢取流量/现金/CSDN周边激励大奖