

BUUCTF: 百里挑一

原创

末初 于 2020-04-07 20:23:26 发布 2065 收藏 2

分类专栏: [CTF_MISC_Writeup](#)

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/mochu777777/article/details/105372624>

版权



[CTF_MISC_Writeup 专栏收录该内容](#)

246 篇文章 45 订阅

订阅专栏

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_f9:97:74 (00:0c:29:f9:97:74)
Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.18
Transmission Control Protocol, Src Port: 9739, Dst Port: 80, Seq: 0, Len: 0

0000 00 0c 29 f9 97 74 00 50 56 c0 00 08 08 00 45 00 ..) t P VE
0010 00 24 36 48 40 00 40 06 b7 17 00 00 64 01 00 00

https://blog.csdn.net/mochu777777

全是在传图片时候的流量，先把图片保存出来

文件 -> 导出对象 -> HTTP -> 保存到一个文件夹

然后使用kali下的 exiftool 找到了一半flag

```
root@mochu7:~/Desktop/test# exiftool *|grep flag
XP Comment : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
root@mochu7:~/Desktop/test# ls
'0(2).jpg' '108(2).jpg' '115(4).jpg' '126.jpg' '14(4).jpg' '163.jpg' '19(2).jpg' '26(4).jpg' '34(2).jpg'
'0(4).jpg' '108(4).jpg' '115.jpg' '127.jpg' '145.jpg' '164.jpg' '19(4).jpg' '26.jpg' '34(4).jpg'
'0.jpg' '108.jpg' '116(2).jpg' '128.jpg' '146.jpg' '16(4).jpg' '19.jpg' '27(2).jpg' '34.jpg'
'100(2).jpg' '109(2).jpg' '116(4).jpg' '129.jpg' '147.jpg' '165.jpg' '1.jpg' '27(4).jpg' '3(4).jpg'
'100(4).jpg' '109(4).jpg' '116.jpg' '12.jpg' '148.jpg' '166.jpg' '20(2).jpg' '27.jpg' '35(2).jpg'
'100.jpg' '109.jpg' '117(2).jpg' '1'(2).jpg' '149.jpg' '167.jpg' '20(4).jpg' '28(2).jpg' '35(4).jpg'
'101(2).jpg' '10.jpg' '117(4).jpg' '130.jpg' '14.jpg' '168.jpg' '20.jpg' '28(4).jpg' '35.jpg'
'101(4).jpg' '110(2).jpg' '117.jpg' '131.jpg' '1'(4).jpg' '169.jpg' '21(2).jpg' '28.jpg' '36(2).jpg'
'101.jpg' '110(4).jpg' '118(2).jpg' '132.jpg' '150.jpg' '16.jpg' '21(4).jpg' '29(2).jpg' '36(4).jpg'
'102(2).jpg' '110.jpg' '118(4).jpg' '13(2).jpg' '151.jpg' '170.jpg' '21.jpg' '29(4).jpg' '36.jpg'
'102(4).jpg' '111(2).jpg' '118.jpg' '133.jpg' '152.jpg' '171.jpg' '22(2).jpg' '29.jpg' '37(2).jpg'
'102.jpg' '111(4).jpg' '119(2).jpg' '134.jpg' '15(2).jpg' '172.jpg' '22(4).jpg' '2.jpg' '37(4).jpg'
'10(2).jpg' '111.jpg' '119(4).jpg' '13(4).jpg' '153.jpg' '17(2).jpg' '22.jpg' '30(2).jpg' '37.jpg'
'103(2).jpg' '112(2).jpg' '119.jpg' '135.jpg' '154.jpg' '173.jpg' '2(2).jpg' '30(4).jpg' '38(2).jpg'
'103.jpg' '112(4).jpg' '111.jpg' '136.jpg' '15(4).jpg' '174.jpg' '23(2).jpg' '30.jpg' '38(4).jpg'
'104(2).jpg' '112.jpg' '120(2).jpg' '137.jpg' '155.jpg' '17(4).jpg' '23(4).jpg' '31(2).jpg' '38.jpg'
'104.jpg' '11(2).jpg' '120.jpg' '138.jpg' '156.jpg' '175.jpg' '23.jpg' '31(4).jpg' '39(2).jpg'
'10(4).jpg' '113(2).jpg' '121(2).jpg' '139.jpg' '157.jpg' '176.jpg' '24(2).jpg' '31.jpg' '39(4).jpg'
'105(2).jpg' '113(4).jpg' '121.jpg' '13.jpg' '158.jpg' '177.jpg' '24(4).jpg' '32(2).jpg' '39.jpg'
'105.jpg' '113.jpg' '122.jpg' '140.jpg' '159.jpg' '178.jpg' '24.jpg' '32(4).jpg' '3.jpg'
'106(2).jpg' '114(2).jpg' '12(2).jpg' '141.jpg' '15.jpg' '179.jpg' '2(4).jpg' '32.jpg' '40(2).jpg'
```

```
106.jpg    114(4).jpg   123.jpg    142.jpg    160.jpg    17.jpg     25(2).jpg   3(2).jpg    40(4).jpg  
'107(2).jpg'  114.jpg    124.jpg    '14(2).jpg'  161.jpg    '18(2).jpg'  '25(4).jpg'  '33(2).jpg'  40.jpg  
'107(4).jpg'  '11(4).jpg'  '12(4).jpg'  143.jpg    162.jpg    '18(4).jpg'  25.jpg     '33(4).jpg'  '41(2).jpg'  
107.jpg    '115(2).jpg'  125.jpg    144.jpg    '16(2).jpg'  18.jpg     '26(2).jpg'  33.jpg     '41(4).jpg'  
root@mochu7:~/Desktop/test# exiftool *|grep flag  
XP Comment : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f  
root@mochu7:~/Desktop/test# █  
https://blog.csdn.net/mochu7777777
```

另外一半在tcp114追踪流当中

过滤器输入: `tcp.stream eq 114`

```
.....m^U^O..~b0R.NJS
.N....g.S.NJS.T..2.6.a.3.c.0.5.8.9.d.2.3.e.d.e.e.c.}.....http://
ns.adobe.com/xap/1.0/.<?xpacket begin='...
id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://
www.w3.org/1999/02/22-rdf-syntax-ns#" /></x:xmpmeta>
```

flag{ae58d0408e26e8f26a3c0589d23edeec}