

CTF——MISC习题讲解（流量分析winshark系列~四）

原创

TJA小傲 于 2022-03-17 14:59:09 发布 1391 收藏 1

分类专栏: [CTF-Misc](#) 文章标签: [web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/lovejr/article/details/123541872>

版权



[CTF-Misc 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

CTF——MISC习题讲解（流量分析winshark系列~四）

前言

上一章节我们已经做完一场流量分析杂项题目, 接下来继续给大家讲解流量分析系列四。

一、工控协议分析

首先打开题目如下

No.	Source	Time	Destination	Protocol	Length	Info
29	192.168.2.53	2.079609	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
30	192.168.2.53	2.079690	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
34	192.168.2.53	2.125538	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
35	192.168.2.53	2.125651	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
39	192.168.2.53	2.171813	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
40	192.168.2.53	2.171904	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
44	192.168.2.53	2.218708	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
45	192.168.2.53	2.218879	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
49	192.168.2.53	2.265692	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
50	192.168.2.53	2.265872	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
54	192.168.2.53	2.313490	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
55	192.168.2.53	2.313576	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
59	192.168.2.53	2.359626	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
60	192.168.2.53	2.359674	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
64	192.168.2.53	2.405832	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
65	192.168.2.53	2.405841	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]

> Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: VMware_b1:29:93 (00:0c:29:b1:29:93), Dst: VMware_1e:c2:d5 (00:0c:29:1e:c2:d5)
> Internet Protocol Version 4, Src: 192.168.2.112, Dst: 192.168.2.53
> Transmission Control Protocol, Src Port: 2810, Dst Port: 102, Seq: 1, Ack: 1, Len: 22
> TPKT, Version: 3, Length: 22
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol

```
0000 00 0c 29 1e c2 d5 00 0c 29 b1 29 93 08 00 45 00  ..).....)....E.  
0010 00 4a 84 44 40 00 40 06 30 74 c0 a8 02 70 c0 a8  .J.D@.@.0t...p.  
0020 02 35 0a fa 00 66 c3 89 25 3b f5 e2 12 3a 80 18  .5...f...%;...:  
0030 fa e7 4a a4 00 00 01 01 08 0a 00 0b 5e 75 00 09  ..J.....^u...  
0040 8d b0 03 00 00 16 02 f0 80 01 00 01 00 61 09 30  .....a.0  
0050 07 02 01 03 a0 02 8b 00  .....
```

CSDN @TJA小傲

搜索flag发现也没有什么有用的东西

其实在做流分题中还是有一个小技巧, 就是看一下长度

排序看到确实有一个长度过于长, 而且在下面也有base编码

No.	Source	Time	Destination	Protocol	Length	Info
1801	192.168.2.53	150.466006	192.168.2.112	TCP	10120	102 → 2817 [PSH, ACK] Seq=1103156 Ack=5906 Win=66560 Len=43 TSval=648217 TSecr=746580 [TCP segment 0
8508	192.168.2.53	393.840663	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8507	192.168.2.53	393.840651	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8505	192.168.2.53	393.840402	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8504	192.168.2.53	393.840294	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8502	192.168.2.53	393.840114	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8501	192.168.2.53	393.839937	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8499	192.168.2.53	393.839792	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8498	192.168.2.53	393.839745	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8496	192.168.2.53	393.839542	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8495	192.168.2.53	393.839506	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8494	192.168.2.53	393.839491	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8492	192.168.2.53	393.839156	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8491	192.168.2.53	393.839089	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8489	192.168.2.53	393.838212	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8488	192.168.2.53	393.838106	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]

> Frame 1801: 10120 bytes on wire (80960 bits), 10120 bytes captured (80960 bits)
 > Ethernet II, Src: Apple_c7:88:1e (60:f8:1d:c7:88:1e), Dst: VMware_b1:29:93 (00:0c:29:b1:29:93)
 > Internet Protocol Version 4, Src: 192.168.2.53, Dst: 192.168.2.112
 > Transmission Control Protocol, Src Port: 102, Dst Port: 2817, Seq: 1103156, Ack: 5906, Len: 43

```

0000 00 0c 29 b1 29 93 60 f8 1d c7 88 1e 08 00 45 00  ..).....E-
0010 00 5f 1b f6 40 00 80 06 58 ad c0 a8 02 35 c0 a8  ..@...X...5-
0020 02 70 00 66 0b 01 44 69 3a a8 c9 75 64 3b 80 18  .p-f...Di :...ud;..
0030 01 04 b9 25 00 00 01 01 08 0a 00 09 e4 19 00 0b  ...%.....
0040 64 54 03 00 1f c6 02 f0 80 01 00 01 00 61 1e 30  dI.....a-0
0050 1c 02 01 03 a0 17 a1 15 02 02 02 0f bf 49 0e 80  .....I-
0060 09 64 61 74 61 20 3d 20 22 64 61 74 61 3a 69 6d  .data = "data:im
0070 61 67 65 2f 70 6e 67 3b 62 61 73 65 36 34 2c 69  age/png; base64,i
0080 56 42 4f 52 77 30 4b 47 67 6f 41 41 41 41 4e 53  VBORw0KG goAAAAANS
0090 55 68 45 55 67 41 41 41 64 41 41 41 41 42 69 43  UhEUGAAA dAAAAABiC
00a0 41 59 41 41 41 44 67 4b 49 4c 4b 41 41 41 41 41  AYAADgK ILKAAAAA

```

CSDN @TJA小傲

No.	Source	Time	Destination	Protocol	Length	Info
1801	192.168.2.53	150.466006	192.168.2.112	TCP	10120	102 → 2817 [PSH, ACK] Seq=1103156 Ack=5906 Win=66560 Len=43 TSval=648217 TSecr=746580 [TCP segment 0
8508	192.168.2.53	393.840663	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8507	192.168.2.53	393.840651	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8505	192.168.2.53	393.840402	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8504	192.168.2.53	393.840294	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8502	192.168.2.53	393.840114	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8501	192.168.2.53	393.839937	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8499	192.168.2.53	393.839792	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8498	192.168.2.53	393.839745	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8496	192.168.2.53	393.839542	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8495	192.168.2.53	393.839506	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8494	192.168.2.53	393.839491	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8492	192.168.2.53	393.839156	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8491	192.168.2.53	393.839089	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8489	192.168.2.53	393.838212	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8488	192.168.2.53	393.838106	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]

> Frame 1801: 10120 bytes on wire (80960 bits), 10120 bytes captured (80960 bits) **物理层**
 > Ethernet II, Src: Apple_c7:88:1e (60:f8:1d:c7:88:1e), Dst: VMware_b1:29:93 (00:0c:29:b1:29:93) **网络接口层**
 > Internet Protocol Version 4, Src: 192.168.2.53, Dst: 192.168.2.112 **IP网络层**
 > Transmission Control Protocol, Src Port: 102, Dst Port: 2817, Seq: 1103156, Ack: 5906, Len: 43 **传输层**

```

0060 09 64 61 74 61 20 3d 20 22 64 61 74 61 3a 69 6d  .data = "data:im
0070 61 67 65 2f 70 6e 67 3b 62 61 73 65 36 34 2c 69  age/png; base64,i
0080 56 42 4f 52 77 30 4b 47 67 6f 41 41 41 41 4e 53  VBORw0KG goAAAAANS
0090 55 68 45 55 67 41 41 41 64 41 41 41 41 42 69 43  UhEUGAAA dAAAAABiC
00a0 41 59 41 41 41 44 67 4b 49 4c 4b 41 41 41 41 41  AYAADgK ILKAAAAA
00b0 58 4e 53 52 30 49 41 72 73 34 63 36 51 41 41 41  XNSR0IAR s4c6QAAA
00c0 41 52 6e 51 55 31 42 41 41 43 78 6a 77 76 38 59  ARNQ1IBA ACXjwv8Y
00d0 51 55 41 41 41 41 4a 63 45 68 5a 63 77 41 41 44  QUAAAAJc Eh2cWAAD
00e0 73 4d 41 41 41 37 44 41 63 64 76 71 47 51 41 41  sMAAA7DA cdvqQAAA
00f0 42 7a 58 53 55 52 42 56 48 68 65 37 5a 32 4a 73  BzXSURBV Hhe7Z21S

```

CSDN @TJA小傲

然后导出分组字节流

No.	Source	Time	Destination	Protocol	Length	Info
1801	192.168.2.53	150.466006	192.168.2.112	TCP	10120	102 → 2817 [PSH, ACK] Seq=1103156 Ack=5906 Win=66560 Len=43 TSval=648217 TSecr=746580 [TCP segment 0
8508	192.168.2.53	393.840663	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8507	192.168.2.53	393.840651	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8505	192.168.2.53	393.840402	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8504	192.168.2.53	393.840294	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8502	192.168.2.53	393.840114	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8501	192.168.2.53	393.839937	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8499	192.168.2.53	393.839792	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8498	192.168.2.53	393.839745	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8496	192.168.2.53	393.839542	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8495	192.168.2.53	393.839506	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8494	192.168.2.53	393.839491	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8492	192.168.2.53	393.839156	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8491	192.168.2.53	393.839089	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8489	192.168.2.53	393.838212	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
8488	192.168.2.53	393.838106	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]

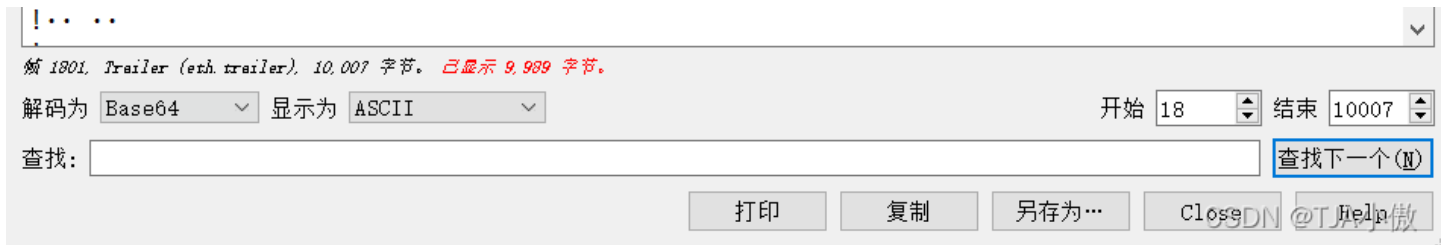
> Frame 1801: 10120 bytes on wire (80960 bits), 10120 bytes captured (80960 bits) **物理层**
 > Ethernet II, Src: Apple_c7:88:1e (60:f8:1d:c7:88:1e), Dst: VMware_b1:29:93 (00:0c:29:b1:29:93) **网络接口层**
 > Internet Protocol Version 4, Src: 192.168.2.53, Dst: 192.168.2.112 **IP网络层**
 > Transmission Control Protocol, Src Port: 102, Dst Port: 2817, Seq: 1103156, Ack: 5906, Len: 43 **传输层**

The image shows a Wireshark packet capture interface. The top pane displays packet details for an Ethernet II frame with source Apple_c7:88:1e and destination VMware_b1:29:93. The second pane shows the Internet Protocol Version 4 details. The third pane shows the raw data in hexadecimal and ASCII. A red arrow points to the ASCII column header. A small dialog box is overlaid on the right side of the packet details pane, showing search options for the selected packet.

这样的话先把对于的东西给去除，然后进行base64解码

The image shows a Wireshark packet capture interface displaying a packet of type 'Trailer (eth.trailer)'. The packet data is shown as a long string of Base64-encoded text. The interface includes search controls at the bottom, such as '开始' (Start) and '结束' (End) fields, and a '查找下一个' (Find Next) button.

The image shows a Wireshark packet capture interface displaying a packet of type 'PNG'. The packet data is shown as a long string of Base64-encoded text, which is the raw data of a PNG image. The interface includes search controls at the bottom, such as '开始' (Start) and '结束' (End) fields, and a '查找下一个' (Find Next) button.



发现是个图片，那就直接在这里转换为图片



得到flag{ICS-mms104}

二、管理员的密码就是flag啊

这个只要读懂题，其实没有什么好讲的

首先打开题目发现以下界面

Wireshark capture showing network traffic. The packet list shows several TCP and DNS packets. The selected packet (No. 10) is an HTTP OPTIONS request from 192.168.1.102 to 115.231.236.116. The packet details pane shows the following information:

- Frame 10: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface 0
- Ethernet II, Src: Tp-LinkT_a6:82:df (80:09:17:a6:82:df), Dst: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 115.231.236.116
- Transmission Control Protocol, Src Port: 4444, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
- Hypertext Transfer Protocol
- Options: /v.gif?pid=307&type=3075&l=47365&t=0&s=47365&v=605&f=12000&n=http%3A%2F%2Fwww.wooyun.org%2F...

Hex dump of the captured packet data. The data is shown in hexadecimal and ASCII. The ASCII column shows the beginning of the packet structure, including the Ethernet II header and the IP header.

管理员密码，那就直接搜索一下flag看看就行

Wireshark capture with a search filter 'password' applied. The packet list shows several HTTP and DNS packets. The selected packet (No. 20) is an HTTP POST request from 192.168.1.102 to 115.231.236.116. The packet details pane shows the following information:

- Frame 20: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits) on interface 0
- Ethernet II, Src: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98), Dst: Tp-LinkT_a6:82:df (80:09:17:a6:82:df)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 115.231.236.116
- Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 1, Ack: 1, Len: 809
- Hypertext Transfer Protocol
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 65
- Form item: "email" = "flag"
- Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd" (highlighted with a red arrow)
- Form item: "captcha" = "BYUG"

The hex dump at the bottom shows the raw data of the packet, with the password field highlighted by a red arrow.

就很简单的得到了flag

flag{ffb7567a1d4f4abdfdb54e022f8facd}

三、getshell

首先打开题目如下

CTF.pcapng

应用显示过滤器: <Ctrl-/>

No.	Source	Time	Destination	Protocol	Length	Info
1	192.168.116.159	0.000000	192.168.116.2	NBNS	110	Refresh NB <01><02> _MSBROWSE <02><01>
2	VMware_c0:00:08	0.640205	Broadcast	ARP	42	Who has 192.168.116.2? Tell 192.168.116.1
3	VMware_c0:00:08	2.039844	Broadcast	ARP	42	Who has 192.168.116.2? Tell 192.168.116.1
4	VMware_c0:00:08	2.640022	Broadcast	ARP	42	Who has 192.168.116.2? Tell 192.168.116.1
5	192.168.116.138	3.062223	91.189.94.4	NTP	90	NTP Version 4, client
6	91.189.94.4	3.440397	192.168.116.138	NTP	90	NTP Version 4, server
7	VMware_c0:00:08	3.640410	Broadcast	ARP	42	Who has 192.168.116.2? Tell 192.168.116.1
8	VMware_ca:16:94	8.050266	VMware_f1:eb:e0	ARP	60	Who has 192.168.116.2? Tell 192.168.116.138
9	VMware_f1:eb:e0	8.050294	VMware_ca:16:94	ARP	42	192.168.116.2 is at 00:50:56:f1:eb:e0
10	192.168.116.138	18.581648	192.168.116.159	ICMP	98	Echo (ping) request id=0xa6f7, seq=1/256, ttl=64 (reply in 11)
11	192.168.116.159	18.581742	192.168.116.138	ICMP	98	Echo (ping) reply id=0xa6f7, seq=1/256, ttl=128 (request in 10)
12	192.168.116.138	19.582551	192.168.116.159	ICMP	98	Echo (ping) request id=0xa6f7, seq=2/512, ttl=64 (reply in 13)
13	192.168.116.159	19.582629	192.168.116.138	ICMP	98	Echo (ping) reply id=0xa6f7, seq=2/512, ttl=128 (request in 12)
14	192.168.116.138	20.583601	192.168.116.159	ICMP	98	Echo (ping) request id=0xa6f7, seq=3/768, ttl=64 (reply in 15)
15	192.168.116.159	20.583748	192.168.116.138	ICMP	98	Echo (ping) reply id=0xa6f7, seq=3/768, ttl=128 (request in 14)
16	192.168.116.138	21.584720	192.168.116.159	ICMP	98	Echo (ping) request id=0xa6f7, seq=4/1024, ttl=64 (reply in 17)

> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface {0E3193A0-2793-4FB9-BE6E-7D2FE6898F28}, id 0
> Ethernet II, Src: VMware_62:1f:55 (00:0c:29:62:1f:55), Dst: VMware_f1:eb:e0 (00:50:56:f1:eb:e0)
> Internet Protocol Version 4, Src: 192.168.116.159, Dst: 192.168.116.2
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service

```
0000 00 50 56 f1 eb e0 00 0c 29 62 1f 55 08 00 45 00  .PV.....)b.U..E.  
0010 00 60 12 eb 00 00 80 11 bd af c0 a8 74 9f c0 a8  ..t.....t...  
0020 74 02 00 89 00 89 00 4c c2 14 80 6b 40 00 00 01  t.....L...k@..  
0030 00 00 00 00 00 01 20 41 42 41 43 46 50 46 50 45  ....A BACFPFPE  
0040 4e 46 44 45 43 46 43 45 50 46 48 46 44 45 46 46  NFDECFC PFHFDEFF  
0050 50 46 50 41 43 41 42 00 00 20 00 01 c0 0c 00 20  PFPACAB.....  
0060 00 01 00 04 93 e0 00 06 e0 00 c0 a8 74 9f  ....t..
```

CSDN @TJA小傲

搜索flag都没有什么用，但是在压缩包里发现了还有一个txt文档

readme.txt - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

1040 4444端口

主要是用来反弹shell的

看下tcp流量

CTF.pcapng

tcp.stream eq 1735

No.	Source	Time	Destination	Protocol	Length	Info
5562	192.168.116.138	364.006055	192.168.116.159	TCP	66	35880 → 1234 [ACK] Seq=24 Ack=822 Win=32768 Len=0 TSval=1664223 TSecr=167733
5574	192.168.116.138	407.125895	192.168.116.159	TCP	106	35880 → 1234 [PSH, ACK] Seq=24 Ack=822 Win=32768 Len=40 TSval=16750 TSecr=167738
5575	192.168.116.159	407.179724	192.168.116.138	TCP	107	1234 → 35880 [PSH, ACK] Seq=822 Ack=64 Win=64177 Len=41 TSval=30581 TSecr=167743
5576	192.168.116.138	407.179800	192.168.116.159	TCP	66	35880 → 1234 [ACK] Seq=64 Ack=863 Win=32768 Len=0 TSval=1675039 TSecr=167748
5604	192.168.116.138	416.358405				
5605	192.168.116.159	416.500475				
5606	192.168.116.138	416.549906				
5607	192.168.116.159	416.720092				
5608	192.168.116.138	416.742003				
5609	192.168.116.159	416.939262				
5610	192.168.116.138	416.941946				
5611	192.168.116.159	417.158669				
5616	192.168.116.138	418.919245				
5617	192.168.116.159	418.919372				
5618	192.168.116.159	418.920687				
5619	192.168.116.138	418.920758				

> Frame 5617: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface {0E3193A0-2793-4FB9-BE6E-7D2FE6898F28}, id 0
> Ethernet II, Src: VMware_ca:16:94 (00:0c:29:ca:16:94), Dst: VMware_f1:eb:e0 (00:50:56:f1:eb:e0)
> Internet Protocol Version 4, Src: 192.168.116.159, Dst: 192.168.116.138
> Transmission Control Protocol, Src Port: 35880, Dst Port: 1234, Seq: 64, Len: 0

Wireshark · 追踪 TCP 流 (tcp.stream eq 1735) · CTF.pcapng

```
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\>ls  
ls  
'ls' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is B03C-791A  
  
Directory of C:\  
  
04/14/2016 08:50 PM          0 AUTOEXEC.BAT  
04/14/2016 08:50 PM          0 CONFIG.SYS  
  
04/14/2016 08:52 PM    <DIR>          Documents and Settings  
02/12/2012 10:34 PM    61,454 bytes     ...
```

```

0000 00 0c 29 62 1f 55 00 0c 29 ca 16 94 08 00
0010 00 34 3b 14 40 00 40 06 95 35 c0 a8 74 8a
0020 74 9f 8c 28 04 d2 47 94 fc c6 2a 38 0b 19
0030 00 20 ee e0 00 00 01 01 08 0a 00 19 9a 97

```

发现这是个winxp的系统，在下面发现了base64编码的

Wireshark · 追踪 TCP 流 (tcp.stream eq 1735) · CTF.pcapng

```

Directory of C:\
04/14/2016 08:50 PM          0 AUTOEXEC.BAT
04/14/2016 08:50 PM          0 CONFIG.SYS

04/14/2016 08:52 PM    <DIR>      Documents and Settings
03/12/2012 10:24 PM    61,454 nc.exe
04/14/2016 08:54 PM    <DIR>      Program Files
04/14/2016 09:22 PM          36 s4cr4t.txt
04/14/2016 08:59 PM    <DIR>      WINDOWS
          4 File(s)      61,490 bytes
          3 Dir(s)  17,719,083,008 bytes free

C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"

```

分组 5555. 0 客户端 分组, 1 服务器 分组, 9 turn(s). 点击选择.

整个对话 (929 bytes) Show data as ASCII 流 1735

查找: 查找下一个(N)

滤掉此流 打印 另存为... 返回 Close Help

米斯特安全团队CTFcrackToolsv2.2 Beta

密码 进制转换 插件 妹子 帮助

Crypto Image UnZip

填写所需解密密码 已输入的字符数:36

Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==

结果 字符数:25

CCTF{do_you_like_sniffer}

CSDN @TJA小傲

最终得到flag

CCTF{do_you_like_sniffer}

目前流量分析的题就到这里结束了，后续有时间也会给大家陆续更新一些杂项其他题目~
估计这几天就开始做靶场了，也会陆续给大家更新的