将嗅探器跟踪转换为MPEG(视频)文件,可通 过VLC查看

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>问题:将嗅探器跟踪转换为MPEG并使用VLC查看</u> <u>解决方案</u> <u>在MPEG中转换数据包</u> <u>将MPEG跟踪转换为可视视频文件</u> 如何使用Wireshark打开任何MPEG视频?

简介

本文档介绍如何将包含MPEG流量的嗅探器跟踪转换为可通过VLC观看的视频。

先决条件

要求

Cisco 建议您了解以下主题:

- Wireshark
- MPEG
- VLC

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

在此特定情况下,数据包捕获在cBR8和RPHY之间进行,并转换为可通过VLC查看的视频流。

其目标不仅是喜欢在工作场所观看专业原因的视频,还要见证视频流中的质量问题,如像素化(宏 屏蔽或拼贴问题)。

问题:将嗅探器跟踪转换为MPEG并使用VLC查看

Wireshark可能无法自动将流量识别为MPEG流量,例如,如果流量被采用在电缆调制解调器终端系统(CMTS)和远程PHY设备(RPD)之间的链路上,它可能会将流量解码为UEPI:

			📮 Sh	ort_mpeg.pcap		
4 1 1 0		C 9 + +	8 7 4 EU	= Q Q Q I	*	
Apply a display filte					-	T Expression +
No.	Time	Source	Destination	Protocol	Length Info	
THE .	1 0,000000	10,243,192,82	10,243,192,78	UEPI	1358 UEPI-DIAG	
	2 0.009388	18,243,192,82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	3 0.047005	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	4 0.047022	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	5 0.077748	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	6 0.077890	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	7 0.082369	10.243.192.82	18.243.192.78	UEPI	1358 UEPI-DIAG	
	8 0.086907	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	9 0.091919	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	10 0.094112	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	11 0.09R878	18.243.192.82	18.243.192.78	UEPT	1358 UEPT-DTAG	
Frame 1: 1358 D Ethernet II, Sr Internet Protoc PSP Header	rytes on wire (10 rc: CiscoInc_11:3 rol Version 4, Sro	864 D1(5), 1358 Dytes 6:13 (78:ba:f9:11:36: c: 10.243.192.82, Dst	captured (10864 bits) 13), Dst: 00:27:90:0aid : 10.243.192.78	12:12 (00:27:90:0a:d2:	f2)	
0000 00 27 90 0a 0010 05 40 00 00 0010 05 40 00 00 0020 c0 4e 00 13 0030 3c c9 0e ac 0040 c3 6f 15 33 0050 056 0f 64 c2 a7 0070 f3 24 3a b1 0080 0c db c5 4e 0090 6c 48 75 62 0060 3f f1 5 3a 0050 6f 15 3a 0060 6f dc 2a 74 0050 6f dc 3a 11 25 0060 6f dc 2a 74 0016 076 f2 4a b1 0016 75 ea c4	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$.'x6E. 			
O 7 Short_more					Packets: 70304 - Displayed: 70304 (10)	0.0%) - Load time: 0:3.56 Profile: Default

解决方案

在MPEG中转换数据包

步骤1.选择UEPI数据包,在数据包详细信息视图中右键点击PSP报头,然后点击解码为。

步骤2.在"当前"菜单下,在协议列表中选择UDP并单击"确定"。

您现在看到UDP数据包(Wireshark可能将其解码为任何其他UDP协议,具体取决于端口号,如果 您仍然看不到MPEG数据包,请继续下一步)。

步骤3.选择UDP数据包,右键单击协议报头,然后选择解**码为。**

步骤4.在"当前"菜单下,在协议列表中选择MP2T,然后单击"确定"

之后,您将看到MPEG数据包,如图所示:

			📮 Sho	rt_mpeg.pcap		
1 1 2	🛛 🗖 🔁	🕹 ۹ 🍝 🔸	2 T 1 🗐 🛙	🗐 Q Q Q 🎹		
Apply a display 1	filter <%/>					Expression +
No.	Time	Source	Destination	Protocol	Length Info	
1	15 0.108201	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a reass	embled packet]
	16 0.108540	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	17 0.112934	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	18 0.115269	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a reass	embled packet] Program _
	19 0.115706	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	20 0.116250	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	21 0.117028	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	22 0.117624	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a reass	embled packet]
	23 0.119800	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	24 0.120631	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet	
	25 8.121268	18.243.192.82	18.243.192.78	MPEG TS	1358 NULL packet	
> User Datagra	m Protocol, Src Port	t: 19 (19), Dst Port:	e (e)			
TSO/IEC 1381	8-1 PID=0x1fff CC=0					
⊨ Header: 0;	<471fff10					
v ISO/IEC 1381	8-1 PID=0x1fff CC=0					
⊨ Header: 0)	<471fff10					
v ISO/IEC 1381	8-1 PID=0x1fff CC=0					
▹ Header: 0;	<471fff10					
ISO/IEC 1381	8-1 PID=0x131 CC=6 :	skips=2				
⊨ Header: 8)	(47013116					
(MPEG2 PCF)	R Analysis]					
⊨ [Expert	Info (Error/Malfor	ned): Detected 2 miss:	ing TS frames before th	is (last_cc:3 total sk:	ips:902 discontinuity:361)]	
[TS Con	tinuity Counter Skip	ps: 2]				
[Some f	rames dropped: 1]					
Reassembled	in: 33					
v ISO/IEC 1381	8-1 PID=@x0 CC=5					
⊨ Header: 8x	47488815					
[MPEG2 PCF	R Analysis]					
Pointer: 6)					
0000 88 27 98	0a d2 f2 78 ba f9	11 36 13 08 00 45 80	.'x6E.			
0010 05 40 00	00 40 00 fd 73 e1	43 0a f3 c0 52 0a f3	.@@s .CR			
0020 c0 4e 00	13 00 00 40 00 30	93 47 1f ff 10 da 01	.N@. 0.G			
0030 60 57 60	17 40 C9 07 40 00 89 b4 36 f9 b1 07	22 12 12 14 42 b4 82	6 3 P			
0050 d8 ac db	ee 97 92 8e 9c d1	99 d9 db d7 7a 4b fd				
0060 27 51 24	11 68 6d f1 63 2e	66 26 24 28 85 68 85	'0\$.hm.c .f&\$(.h.			
0070 b1 5d b7	dd 2f 24 1d 39 a3	33 b3 b7 ac f4 97 fa	.1/\$.9 .3			
0080 4e a2 48	22 d0 db e2 c6 5c	cc 4c 48 51 8b d8 8b	N.H" \.LHQ			
0090 62 bb 6f	ba 5e 48 3a 73 46	67 67 6f 5d e8 2f f4	b.o.^H:s Fggo]./.			
0000 90 44 98	45 81 07 C5 8C 09 74 bc 98 74 86 8c	90 90 90 az 1/ a0 10	v t t			
00c0 3a 89 20	8b 43 6f 8b 19 73	31 31 21 44 2e 40 2d	:Co s11!D.@-			
0 7 that are					Barbara 20204 - Disclosed 20204 (100 off) - 1	and Kime (0.0.200) Depline Defects
- snort_mp	e				Packets: 70304 - Displayed: 70304 (100.0%) - D	Protie: 012.739 Protie: Detault

为了将数据包正确解码为MPEG,您可以观看以下视频:

将MPEG跟踪转换为可视视频文件

步骤1.安装LUA MPEG DUMP Wireshark插件,可从以下位置获得:mpeg_dump.lua。

对于MAC OS用户,可以在上述链接的页面下载名为mpeg_packets_dump.lua的插件,并将其移动 到路径中:/Applications/Wireshark.app/Contents/Resources/share/wireshark。

在同一文件夹中,在名为init.lua的文件末尾附加一行<dofile("mpeg_packets_dump.lua")>。

步骤2.您现在必须在Wireshark中看到新项目,导航至"工具">"转储MPEG TS数据包",如图所示:

Tools	Help
Dum	p MPEG TS Packets
Lua	►]

选择它,然后输入文件名,如果只想提取流的某些部分(例如,如果流包含多个PID),最终输入 过滤器。

这将创建一个.ts文件,可通过VLC作为视频流查看:



此图像故意显示视频拼贴,以显示此过程如何确实有助于发现视频流问题。

如何使用Wireshark打开任何MPEG视频?

作为副主题,Wireshark支持任何MPEG视频文件并正确显示MPEG数据包(当然,不包含任何IP报 头,因为本地文件中没有任何IP报头):

	tovideo.ts	_					
📕 📕 🖉 🔘 🔲 🗋 🗙 🙆 🥄 🦛 🏓 🔜 🖌 👤 🛄	📃 0, 0, 0, 🖞	L					
Apply a display filter <%/>		Expression	+				
No. Time Source Destination	Protocol	Length Info	_				
6 0.003778518	MPEG TS	188 [MP2T fragment of a reassembled packet]					
7 0.004534222	MPEG TS	188 (MP2T fragment of a reassembled packet)					
8 0.005289925	MPEG TS	188 [MP2T fragment of a reassembled packet]					
9 0.006045629	MPEG TS	188 [MP2T fragment of a reassembled packet]					
10 0.006801333	MPEG TS	188 [MP2T fragment of a reassembled packet]					
11 0.007557037	MPEG TS	188 [MP2T fragment of a reassembled packet]					
12 0.008312740	MPEG TS	188 (MP2T fragment of a reassembled packet)					
13 0.009068444	MPEG TS	188 [MP2T fragment of a reassembled packet]					
14 0.009824148	MPEG TS	188 Program Association Table (PAT)					
15 0.010579851	MPEG TS	188 [MP2T fragment of a reassembled packet]					
16. 0.011335555	MPEG TS	188 [MP2T fragment of a reassembled packet]	_				
▷ Frame 14: 188 bytes on wire (1584 bits), 188 bytes captured (1584 bits)							
▶ ISO/IEC 13818-1 PID=0x0 CC=4							
v MPEG2 Program Association Table							
Table ID: Program Association Table (PAT) (0x00)							
1 = Syntax indicator: 1							
.011 = Reserved: 0x0003							
0000 0001 0001 = Length: 17							
Transport Stream ID: 0xa8a0							
11 = Reserved: 0x03							
11 101. = Version Number: 0x1d							
Section Number: 0							
Lat Series Number 0							
Last actual memory of							
P Program 0x0000 -> PTD 0x0100 Droman 0x0000 -> PTD 0x0100							
P Program execute Provide Country Coun							
v Stuffina							
Stuffing: ffffffffffffffffffffffffffffffffffff							
0000 47 40 00 14 00 00 b0 11 a8 a0 fb 00 00 00 0a c1 G0			-				
0010 30 00 0c e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff ffz							
0020 ff							
eese ff							
DOGD . ff f							
0070 ff							
0000 ff							
0000 ff							
BOBB ff f							
A 7 miles		B	-				

如果要确保源视频文件正确,这非常有用。如果源视频文件包含CC错误,此处没有幻数,则可能一 直存在CC错误。

此外,如果您只能使用DVB-C USB转换器接收视频,它可捕获MPEG数据包并允许将视频流存储为 文件,则此功能也非常有用。然后,您可以使用wireshark重新打开它,以确保其正确。