轉換Wireshark的存取點資料包轉儲

目錄

<u>簡介</u>

<u>必要條件</u>

<u>程式</u>

執行資料包轉儲

<u>輸出檔案清除</u>

<u>清除封包摘要資訊</u>

移除起始空格與位移冒號

<u>正確的資料包偏移</u>

<u>單獨資料包位元組</u>

<u>將文字檔轉換成PCAP</u>

透過Wireshark GUI

汤핵壮級

<u>疑難排解</u>

<u>文本檔案正確,但Text2pcap無法讀取任何資料包</u>

<u>不一致的位移</u>

透過命令列

簡介

本文檔介紹如何將COS存取點生成的資料包轉儲轉換為Wireshark的PCAP格式,作為解決大小限制 的解決方法。

必要條件

- 記事本++ -僅適用於Windows
- 已安裝Text2pcap -包含在常規安裝的Wireshark中

程式

執行資料包轉儲

透過在AP命令列上運行debug traffic wired <multiple options> verbose命令,捕獲AP資料包轉儲。 您可以在多個過濾器和介面之間選擇。

在終端中記錄會話。

執行此操作時,請小心傳送最少量的按鍵動作,檔案上不屬於擷取本身的可列印字元越多,您在轉 換之前需要執行的清除就越多。

最簡單的方法是進行資料包轉儲的控制檯會話、複製問題、停止轉儲並立即結束會話。

如果透過ssh執行轉儲,請使用過濾器來僅捕獲所需的流量。否則,捕獲包含ssh會話資料包。

有關如何配置捕獲的完整說明,請參閱<u>COS AP故障排除</u>。

完成後,請使用undebug all命令停止捕獲。產生的檔案如下所示:

AP-9105>en Password: AP-9105#debug traffic wired udp capture capture packets in pcap file verbose Verbose Output <cr> AP-9105#debug traffic wired udp verbose AP-9105#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656 0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500 0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff 0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20 0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e 0x0040: 636f 6469 6e67 3d22 7574 662d 3822 3f3e <truncated> undebug 0x0070: 444c 4e41 444f 432f 312e 3530 2050 6c61 0x0080: 7469 6e75 6d2f 312e 302e 342e 320d 0a4d 0x0090: 414e 3a20 2273 7364 703a 6469 7363 6f76 0x00a0: 6572 220d 0a53 543a 2073 7364 703a 616c 0x00b0: 6c0d 0a4d 583a 2033 0d0a 0d0a a11 <truncated> tcpdump: pcap_loop: error reading dump file: Interrupted system call All possible debugging has been turned off <end of file>

輸出檔案清除

刪除不屬於資料包轉儲本身的任何資訊。刪除檔案中包含dump命令、包含主機名(APname#)的任何 提示以及任何其他不相關的系統日誌消息的行。

請特別注意undebug命令,因為它可以在資料包內容之前列印,如上所示。清理後,產生的檔案如 下所示:

清除封包摘要資訊

當出現新的偏移000000時,會檢測到新資料包的開始。Text2pcap可以處理每個資料包之前列印的 摘要資訊,以避免出現最適合刪除它們的問題。

在記事本中++導航到搜尋>查詢,然後選擇標籤頁籤,確保搜尋模式為擴展。

在「查詢內容:」欄位中,輸入符號>,然後按一下「全部標籤」。此動作會將包含>符號的所有行 加入書籤。

Mark		×
Find Replace Find in Files Find in Projects Mark		
Eind what: 📘	v	Mark All
		Clear all marks
Bookmark line	In selection	Copy Marked Text
Backward direction		Close
Match whole word only		
Match gase		
Wrag around		
Search Mode		C Transparency
Normal		On losing focus
Extended (\n, \r, \t, \0, \x)		Always
Regular expression matches newline		

記事本++標籤通話方塊,並尋找內含Chevron字元的欄位。

標示頁首後,記事本++會反白所有檔案明細行,如下所示:

		of the second of the second of the second of the		P debug mice sample copylog E
1 🔵	22:35:17.1669188	IP CSCO-W-PF320YP6.lan.60354	239.255.255.250.3702: UDP, length 656	
	0x0000:	0100 5e7f fffa 806d 971d a040	0800 4500	
	0x0010:	02ac d4bb 0000 0111 cd11 c0a8	64d1 efff	
	020020.	fffa abc2 0a76 0208 757h 3c3f	7864 6620	

突出顯示的包含Chevron的行的資料包轉儲代碼段。

·導航到搜尋>書籤,然後按一下刪除帶書籤的行。執行此操作後,檔案看起來與以下代碼段類似:

0x0000:01005e7ffffa806d971da040080045000x0010:02acd4bb00000111cd11c0a864d1efff0x0020:fffaebc20e760298757b3c3f786d6c200x0030:76657273696f6e3d22312e302220656e

移除起始空格與位移冒號

導航到搜尋>查詢,選擇替換頁籤,確保搜尋模式為擴展。

在查詢內容:欄位中輸入8個空格。將替換為:欄位保留為空,然後按一下全部替換。這樣會將每行 開頭的所有8個連續空白取代為空白,有效地刪除它們。「取代」通話方塊看起來就像此影像。

Replace		×
Find Replace Find in Files Find in Projects Mark		
Eind what:		🔺 🔍 🔻 Find Next
Rep <u>l</u> ace with:		<u>R</u> eplace
	In selection	Replace <u>A</u> ll
Backward direction		Replace All in All Opened Doc <u>u</u> ments
Match case		Close
🗹 Wrag around		
Search Mode	21	Transparenc <u>y</u>
<u>N</u> ormal		 On losing focus
Extended (\n, \r, \t, \0, \x)		 Always
Regular expression matches newline		
Replace All: 2935 occurrences were replaced in entir	e file	

記事本++用「查詢包含8個空格的欄位」替換對話方塊。

此操作後生成的檔案類似於以下代碼段:

0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500 0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff 0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20

x0030: 7	0: 7665 727	3 696f 6e3	d 2231 2e30	2220 656e
x0040:	0: 636f 646	9 6e67 3d2	2 7574 662d	3822 3f3e
x0050:	0: 3c73 6f6	1 703a 456	e 7665 6c6f	7065 2078
x0060:	0: 6d6c 6e7	3 3a73 6f6	1 703d 2268	7474 703a
x0070: 2	0: 2f2f 777	7 772e 773	3 2e6f 7267	2f32 3030
x0040: x0050: x0060: x0070:	0: 6367 646 0: 3c73 6f6 0: 6d6c 6e7 0: 2f2f 777	9 6e67 3d2 1 703a 456 3 3a73 6f6 7 772e 773	2 7574 662d e 7665 6c6f 1 703d 2268 3 2e6f 7267	3822 31 7065 20 7474 70 2f32 30

導航到搜尋>查詢,選擇替換頁籤,確保搜尋模式為擴展。在查詢內容:欄位中輸入:(請注意冒號 後面的空格)。將「替換為:」欄位保留為空,然後按一下「全部替換」。 這樣會取代位移後的所有冒號和第一個空格。

			_
Replace			\times
Find Replace Find in Files Find in Projects Mark			
Eind what:		▲ ▼ Find Next	
Replace with:		<u>R</u> eplace	
	In selection	Replace <u>A</u> ll	
Backward direction		Replace All in All Opened Doc <u>u</u> ments	
Match whole word only		Close	
Wrap around			
Search Mode	v 1	Transparency	
<u>N</u> ormal		 On losing focus 	
Extended (\n, \r, \t, \0, \x)		Always	
Regular expression matches newline			
Replace All: 2935 occurrences were replaced in entire file			.:

記事本++「取代」通話方塊為「尋找以冒號與空格填入的欄位」。

在先前的操作之後,產生的輸出檔案看起來就像這個程式碼片段:

0x000001005e7ffffa806d971da040080045000x001002acd4bb00000111cd11c0a864d1efff0x0020fffaebc20e760298757b3c3f786d6c200x003076657273696f6e3d22312e302220656e0x0040636f64696e673d227574662d38223f3e0x00503c736f61703a456e76656c6f706520780x00606d6c6e733a736f61703d22687474703a0x00702f2f7777772e77332e6f72672f323030

正確的資料包偏移

Text2pcap期望每個資料包內的資料包偏移量是一個6個字元的十六進位制字串,但AP資料包轉儲使 用0x來表示偏移。要更正此問題,請導航到搜尋>查詢,然後選擇替換頁籤,確保搜尋模式為擴展 。

在「查詢內容:」欄位中輸入x。將替換為:欄位填入0,然後按一下全部替換。如此會以0取代位 移內的所有x,以符合Text2pcap的預期位移格式。

Replace		×
Find Replace Find in Files Find in Projects Mark		
<u>F</u> ind what: x		🔺 🔍 🔻 Find Next
Rep <u>l</u> ace with: 0	v ····	<u>R</u> eplace
	In select <u>i</u> on	Replace <u>A</u> ll
Backward direction		Replace All in All Opened Documents
Match <u>w</u> hole word only Match <u>c</u> ase		Close
✓ Wrap around		
Search Mode	т 🔁	ransparenc <u>y</u>
Normal		On losing focus
Extended (\n, \r, \t, \0, \x)		Always
Regular expression matches newline		
Replace All: 2935 occurrences were replaced in entire fil		

記事本++「取代」對話方塊中的「尋找填入字元x的欄位」和「取代」欄位中的字元0填入的欄位。

在先前的操作之後,產生的輸出檔案看起來就像這個程式碼片段:

00000001005e7ffffa806d971da0400800450000001002acd4bb00000111cd11c0a864d1efff000020fffaebc20e760298757b3c3f786d6c2000003076657273696f6e3d22312e302220656e00040636f64696e673d227574662d38223f3e000503c736f61703a456e76656c6f70652078

單獨資料包位元組

Text2pcap資料格式要求每對十六進位制值用空格分隔,不正確的格式會導致Text2pcap將資料包資料讀取為偏移量並失敗。

導航到搜尋>查詢,然後選擇替換頁籤,確保搜尋模式為正規表示式。

在「尋找內容」欄位上輸入([0-9a-f][0-9a-f])([0-9a-f][0-9a-f])(請注意前導空格)。

將替換為:欄位填入\1 \2(請注意前導空格),然後按一下全部替換。

替換操作將查詢資料包的十六進位制位元組並在每對之間插入一個空格。正規表示式匹配後跟一個 十六進位制數字對的空格,將其儲存在捕獲組1中,然後獲取相鄰十六進位制數字對,將其儲存在捕 獲組2中。取代項會列印必要的空格以及每個擷取群組的內容。

視檔案的長度而定,此過程需要數秒或數分鐘。它在運行時會佔用大量RAM。如果檔案很大,請耐 心等待。

Replace	×
Find Replace Find in Files Find in Projects Mark	
Find what: ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f])	🖌 🚺 🔽 Find Next
Replace with: \1 \2	<u>R</u> eplace
In selection	Replace <u>A</u> ll
Backward direction	Replace All in All Opened
Match whole word only	
Match <u>c</u> ase	Close
✓ Wrap around	
Search Mode	
<u>N</u> ormal	 On losing focus
Extended (\n, \r, \t, \0, \x)	Always
Regular expression In the set of th	

記事本++「取代」通話方塊中會顯示以規則運算式填入的搜尋專案,以及以其他規則運算式填入的「取代」欄位。

在先前的操作之後,產生的輸出檔案看起來就像這個程式碼片段,並且已經可以透過Text2pcap進 行轉換。

 000000
 01
 00
 5e
 7f
 ff
 fa
 80
 6d
 97
 1d
 a0
 40
 08
 00
 45
 00

 000010
 02
 ac
 d4
 bb
 00
 00
 11
 cd
 11
 c0
 a8
 64
 d1
 ef
 ff

 000020
 ff
 fa
 eb
 c2
 0e
 76
 02
 98
 75
 7b
 3c
 3f
 78
 6d
 6c
 20

 000030
 76
 65
 72
 73
 69
 6f
 6e
 3d
 22
 31
 2e
 30
 22
 20
 65
 6e

 000040
 63
 6f
 64
 69
 6e
 67
 3d
 22
 75
 74
 66
 2d
 38
 22
 3f
 3e

 000050
 3c
 73
 6f
 61
 70
 3a
 45
 6e
 76
 65
 6c
 6f
 70
 3a
 3a

 000060
 6d
 6c
 67
 3

將文字檔轉換成PCAP

透過Wireshark GUI

要將完整檔案轉換為pcap,請打開Wireshark並導航到檔案>從十六進位制轉儲導入,此時將顯示一個對話方塊。

	ug wred sa	mple - Copy.log		 Browse
lar Expression				
ecimal il				
0				
21:19:01:19:5.19:F		(No format will b	e applec)	
Ethernet				~
57				
hertype (hex):				
otocol (dec):			IP version:	IPv4 👳
urce address:				
stination address:				
urce port:				
stination port:				
g:				
1:				
	Ethernet colocol (dec): urce address: stination address: stination port:	Ethernet		Image: State of the second

按一下Browse...按鈕並選擇轉儲文本檔案。確保所選的偏移型別為Hexadecimal,Encapsulation type為Ethernet,並且未選擇No dummy header。

按一下Import開始轉換過程。

透過命令列

要在windows命令列中將文本檔案轉換為pcap檔案,請運行<path to wireshark install folder>\text2pcap.exe <path to text file pcap> <output file path>。

您可以選擇將wireshark資料夾增加到PATH中,否則每次轉換檔案時都需要運行text2pcap來引用 text2pcap.exe的整個路徑。Text2pcap.exe位於wireshark安裝資料夾內。



成功進行資料包轉儲轉換後的Windows命令列輸出

Text2pcap還包含多個用於預處理文本檔案的正規表示式選項,有關詳細資訊,請參閱<u>Text2pcap手</u> <u>冊頁</u>。

疑難排解

文本檔案正確,但Text2pcap無法讀取任何資料包

Text2pcap無法讀取常用終端模擬程式(Secure CRT、Putty或其他)生成的某些檔案編碼。 變更為使用記事本++的Text2pcap可讀取的編碼。轉到Encoding>UTF-8並儲存檔案,然後再次轉換 為pcap。

File Edit	Search View	Encoding	Language	Settings	Tools	Macro	Run	Plugin	s Win	dow ?								
) 6 8		ANS	I					⊒ d	, <u>=</u> </td <td>) M (</td> <td>ן f_ג</td> <td>₽⊘</td> <td>\odot</td> <td></td> <td>▶ 🔒 </td> <td>📮 🎫 📰 🤇</td> <td>z 🔺 🛪 🗷</td> <td>l</td>) M (ן f_ג	₽⊘	\odot		▶ 🔒	📮 🎫 📰 🤇	z 🔺 🛪 🗷	l
	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100	• UTF-	8				- 1 M - 1		يم				, _ 				-	
193	000100	UTF- UTF-	8-BOM			a7	76	16	77	5b	02	d8	9c	07	f6	b1		
194	000110	UTF-	16 LE BOM			۱b	fd	15	15	6f	74	d7	f5	6c	30	72		
195	000120	Char	acter sets		>	C	46	1a	20	cd	e3	fb	ef	10	3f	5d		
196	000130	Conv	vert to ANSI			52	9e	03	a4	a7	fd	dØ	3e	d8	18	27		
197	000140	Conv	vert to UTF-8	POM) 3	f9	24	16	b3	57	4f	93	e7	20	e2		
198	000150	Con	vent to UTF-8 vert to UTF-1	6 BE BOM)b	d5	57	64	90	01	72	57	b9	83	6d		
199	000160	Conv	vert to UTF-1	6 LE BOM		}a	6f	f8	b5	ce	8a	8e	9a	a0	9c	42		

記事本++編碼功能表選項。

不一致的位移

當資料包上的資料部分位元組未正確分隔成對時,會出現此錯誤,這將導致Text2pcap假設新資料 包的開始而無法解釋。

搜尋資料包內容中間沒有分隔的任何資料包位元組或字串,例如 undebug all 命令。

:\Users\mariomed>text2pcap "C:\Users\mariomed\Downloads\debug wired sample - Copy.log" output.pcap									
Input from: C:\Users\mariomed\Downloads\debug wired sample - Copy.log									
Dutput to: output.pcap									
Dutput format: pcapng									
** (text2pcap:81244) 10:30:46.781149 [(none) MESSAGE] Inconsistent offset. Expecting 75, got 80. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.781712 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.782136 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.782446 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.782599 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.782748 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.782891 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.783033 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.783169 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.783319 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								
** (text2pcap:81244) 10:30:46.783456 [(none) MESSAGE] Inconsistent offset. Expecting 10, got 10. Ignoring rest of pack	et								

嘗試轉換無效檔案後的Windows命令列輸出。不一致的偏移被多次列印到終端。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。