LWAPP對WildPackets OmniPeek和EtherPeek 3.0軟體進行解碼啟用

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> 慣例 <u>修改LWAPP解碼檔案</u> <u>修改TCP_UDP_Ports.dcd</u> <u>修改Pspecs.xml檔案</u> <u>OmniPeek 5.0中的LWAPP解碼</u> 驗證 相關資訊

<u>簡介</u>

WildPackets OmniPeek(和EtherPeek)具有可用的輕量型存取點通訊協定(LWAPP)解碼,但是它 們沒有插入。本文檔說明如何啟用LWAPP解碼並使用軟體檢視LWAPP。本檔案使用EtherPeek 3.0和OmniPeek 5.0的程式。

註: OmniPeek 3.0的過程與EtherPeek 3.0的過程相同。

注意:OmniPeek和EtherPeek軟體之間的唯一區別是檔案的位置。

- OmniPeek的路徑為C:/Program Files/WildPackets/OmniPeek。
- EtherPeek的路徑為C:/Program Files/WildPackets/EtherPeek。

<u>必要條件</u>

<u>需求</u>

思科建議您瞭解EtherPeek、OmniPeek 3.0和5.0軟體。有關EtherPeek的資訊,請參閱 <u>EtherPeek常見問題</u>。有關OmniPeek的資訊,請參閱<u>Omni簡介</u>。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

OmniPeek 3.0

- EtherPeek 3.0
- OmniPeek 5.0

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

修改LWAPP解碼檔案

要修改LWAPP解碼檔案,請向LWAPP函式新增「ETHER 0 0 90 c2 AP Identity:;」。它直接位於 LWAPP-light_weight_..中的「LABL 0 0 b1 Light Weight Access Point Protocol\LWAPP:;」行下。 protocol.dcd檔案(C:\Program Files\WildPackets\EtherPeek\Decodes)。

修改TCP_UDP_Ports.dcd

在TCP_UDP_Ports.dcd檔案(C:\Program Files\WildPackets\EtherPeek\Decodes)中,必須包含以下 兩行:

0x2fbe | LWAPP;

0x2fbf | LWAPP;

注意:此過程導致主機電腦上沒有開啟任何埠。因此,此步驟不會使主機電腦面臨任何安全風險。

如此一來,兩個連線埠12222和12223都會包括在內。

修改Pspecs.xml檔案

請完成以下步驟:

1. 在檔案pspecs.xml(C:\Program Files\WildPackets\EtherPeek\1033)的「使用者資料包通訊協 定(UDP)」區段中,新增以下行:**注意:**請確保首先備份原始檔案。

```
<PSpec Name="LWAPP">
  <PSpecID>6677</PSpecID>
  <LName>LWAPP</LName>
  <SName>LWAPP</SName>
   <Desc>LWAPP</Desc>
  <Color>color_1</Color>
  <CondSwitch>12222</CondSwitch>
  <CondSwitch>12223</CondSwitch>
    <PSpec Name="LWAPP Data">
<PSpecID>6688</PSpecID>
<LName>LWAPP Data</LName>
<SName>LWAPP-D</SName>
 <DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12222) || (DestPort == 12222)]]></CondExp>
     </PSpec>
     <PSpec Name="LWAPP Control">
<PSpecID>6699</PSpecID>
<LName>LWAPP Control</LName>
 <SName>LWAPP-C</SName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
```

2. 重新啟動OmniPeek或EtherPeek以使更改生效。

<u>OmniPeek 5.0中的LWAPP解碼</u>

OmniPeek版本5.0是OmniPeek版本3.0的下一代捕獲工具。在5.0版本中,LWAPP解碼預設是內建 的。因此,無需對檔案進行任何進一步更改。但是以下示例顯示如何使用IP地址和埠號在5.0版本中 定義協定過濾器:

- 1. 開啟OmniPeek 5.0應用程式。
- 2. 在Start頁中,按一下**File > New**以開啟New Packet Capture Window。出現一個名為「 Capture Options(捕獲選項)」的小視窗。它包含資料包捕獲的選項清單。
- 3. 在Adapter選項中,選擇一個介面卡以使用該介面卡捕獲資料包。突出顯示介面卡時,有關介面卡的說明如下所示。選擇Local Area Connection以使用本地乙太網介面卡捕獲資料包。
- 4. 按一下「OK」(確定)。此時會顯示「新建捕獲」視窗。
- 5. 按一下Start Capture按鈕。該工具開始為軟體中定義的協定捕獲資料包。要檢視捕獲的資料包 ,請按一下左側Capture選單下方的Packets選項。
- 6. 按一下右鍵捕獲的任何資料包,然後按一下**Make Filter**以定義新的協定。出現「Insert Filter(插入過濾器)」視窗。
- 7. 在Filter框中輸入名稱以標識協定。啟用Address過濾器。選擇Type as IP,以捕獲到特定IP地 址或從特定IP地址捕獲的資料包。對於Address1,輸入源IP地址。如果目的地址有靜態IP,則 對於地址2,輸入IP地址。如果目的地通過DHCP收到IP地址,則選擇Option as Any Address。要指定資料包流的方向,請按一下Both direction按鈕並選擇三個選項之一。按鈕上 的箭頭標籤表示所選方向。啟用Port過濾器。為協定使用的埠選擇型別,例如TCP。Port 1輸 入來源中使用的連線埠。如果目的地使用標準且定義良好的連線埠,則為連線埠2輸入連線埠 號碼。否則,如果目的地以隨機方式使用連線埠,請選擇Any port選項。根據您的要求,從兩 個方向按鈕選擇方向。
- 8. 重複以上步驟以定義任何新的自定義協定。

<u>驗證</u>

使用OmniPeek 5.0,您可以從Capture Screen驗證在觸發LWAPP事件時,預設情況下該工具會捕 獲LWAPP協定。<u>圖1顯</u>示LAP發出的發現請求期間的LWAPP協定捕獲。

圖1

Pile Edit View	Capture Send Monitor Tool	s Wedow Help							- 0
🗟 = 😢 = 🗳	N N A 2 4 4	8420001	- P - B	0	a Duy Now				
Packets received	707 Buffer usaget 19% Buffer usaget						and the second	-	
Packets filtered	707 Filter st	tates 🗰 Accept all packets						3.00	Capture
-									
= Capture	A		10 CL	10					1.1
Deshboard	- es m co co				and the second	and the second second	and the second		
Packets	Source	Destination	Plags	524	Relative Tane	Protocol	Summary	1.1.1.1.1.1.1	
Log	3 10.77.244.209	IF Broadcast		96	0:01:10.277675	DW3	C OUERY RAME-CI	SCO-LWAPP-	CONTROL
Filters	#900:1A:A1:54:30:AB	Moast 802.14 Br	•	64	0:01:11.067006	002.1			
Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	syslog	SEC-60909,D#t=	514 ,1-	122
Hierarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	syslog	SIC+60909,D#t+	514 ,1+	95
Flat	3 10.77.244.209	IP Broadcast		137	0:01:11.277584	sistod	SEC-60909,D9t-	514 ,1-	91
Application	00:1A:A1:54:30:AB	Mast 802.1d St	•	64	0:01:13.072054	002.1			
i≡ Web	10.77.244.209	IP Broadcast		96	0:01:13.277035	08/5	C QUERT RAME+CI	SCO-LWAPP-	CONTROL
Servers	B000:1A:A1:54:30:AB	BCast 802.14 Br	•	64	0:01:15.077120	-802.1			
Clerks	3 10.77.244.209	IF Buoadcast		96	0:01:16.275883	04/5	C QUERT NAME-CI	SCO-LWAPP-	CONTROL
Pages	#00:1A:A1:54:30:AB	Reast 802.14 Sr	•	64	0:01:17.081615	002.1			
Requests	B00:1A:A1:54:30:AB	Mcast 802.1d Sr	•	64	0:01:19.088698	802.1			
R Voice & Video	B900:18:D4:E3:A6:18	Etheznet Szondcast		- 64	0:01:19.275905	ARP Request	10.77.244.204 +	2	
Calls	B900:1A:A1:54:30:AB	B) 00:1A:AI:54:30:AB		64	0:01:20.042094	Loopback			
Media	10.77.244.209	IP Brosdcast		151	0:01:20.274075	syslog	SEC-60909,D91+	514 .14	105
R Visuals	10.77.244.209	TP Broadcast		156	0:01:20.275459	syslog	SEC+60909,Dat+	514 ,14	110
Apdex	3 10.77.244.209	🚼 IF Broadcast		146	0:01:20.276394	14435	Szc+14977,Dat+1	2223 yike -	100
Peer Map	2900:1A:A1:54:30:A8	Blast 002.14 St		64	0:01:21.090924	002.1			
Graphs	BOD: 1A:A1: 54: 30:AB	Bast 802.1d Br		64	0:01:23.095938	002.1			
Statistics	B900:1A:A1:54:30:AB	201200100100100100100		64	0:01:23.481099	00-00-00-20-04			
Nodes	200:1A:A1:54:30:A8	E01:00:0C:00:00:00		-94	0:01:23.481160	00-00-00-00-03			
Protocols	#00:1A:A1:54:30:A5	Moast 002.14 BE		64	0:01:25.102850	002.1			
Summary	#00:1A:A1:54:30:AB	Boast 802.1d BE		64	0101127.107696	802.1			
	BOD:1A:A1:54:30:AB	BReast 802.1d Sc		64	0:01:29.112083	802-1			
	200:1A:A1:54:30:A8	\$90011A1A11541301AB		64	0:01:30.051235	Loopback			
	B00:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:30.292150	ARP Request	10.77.244.203 -	7	
	#00:1A:A1:54:30:AB	BRCAFT 002.1d Bc		64	0:01:31.116975	802.1			
	\$900:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:31.291080	ARP Request	10.77.244.203 -	2	
	#900:1A:A1:54:30:A8	BRCAST 802.14 St		64	0:01:33.122176	802.1			
	10.77.244.209	1P Broadcast		132	0:01:34.336071	syslog	drc=60909.Det=	514 .1-	66
	10.77.244.209	IF Broadcast		132	0:01:34,336487	syslog	Szc=60909_Dyt=	514 .1-	64
	\$900:1A:A1:54:30:A8	Boast 802.1d Br		64	0:01:35,126796	802.1			
	10.77.244.209	IP Broadcast		132	0:01:35,348150	syslog	Src-60909.Dat-	514 .1-	66
	00:1A:A1:54:30:A5	BCARL 802.1d Br		64	0:01:37,135293	802.1			
						Ard			
	C. The shares are seen as								

按兩下該資料包以檢視有關該資料包的詳細資訊。

相關資訊

- <u>EtherPeek常見問題</u>
- Omni简介
- <mark>下载OmniPeek 5.0</mark>
- 技術支援與文件 Cisco Systems