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

目錄

簡介

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。

必要條件

需求

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EtherPeek常見問題 。有關OmniPeek的資訊，請參閱Omni簡介 。

採用元件

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

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

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>
```

```
    </PSpec>
</PSpec>
```

2. 重新啟動OmniPeek或EtherPeek以使更改生效。

OmniPeek 5.0中的LWAPP解碼

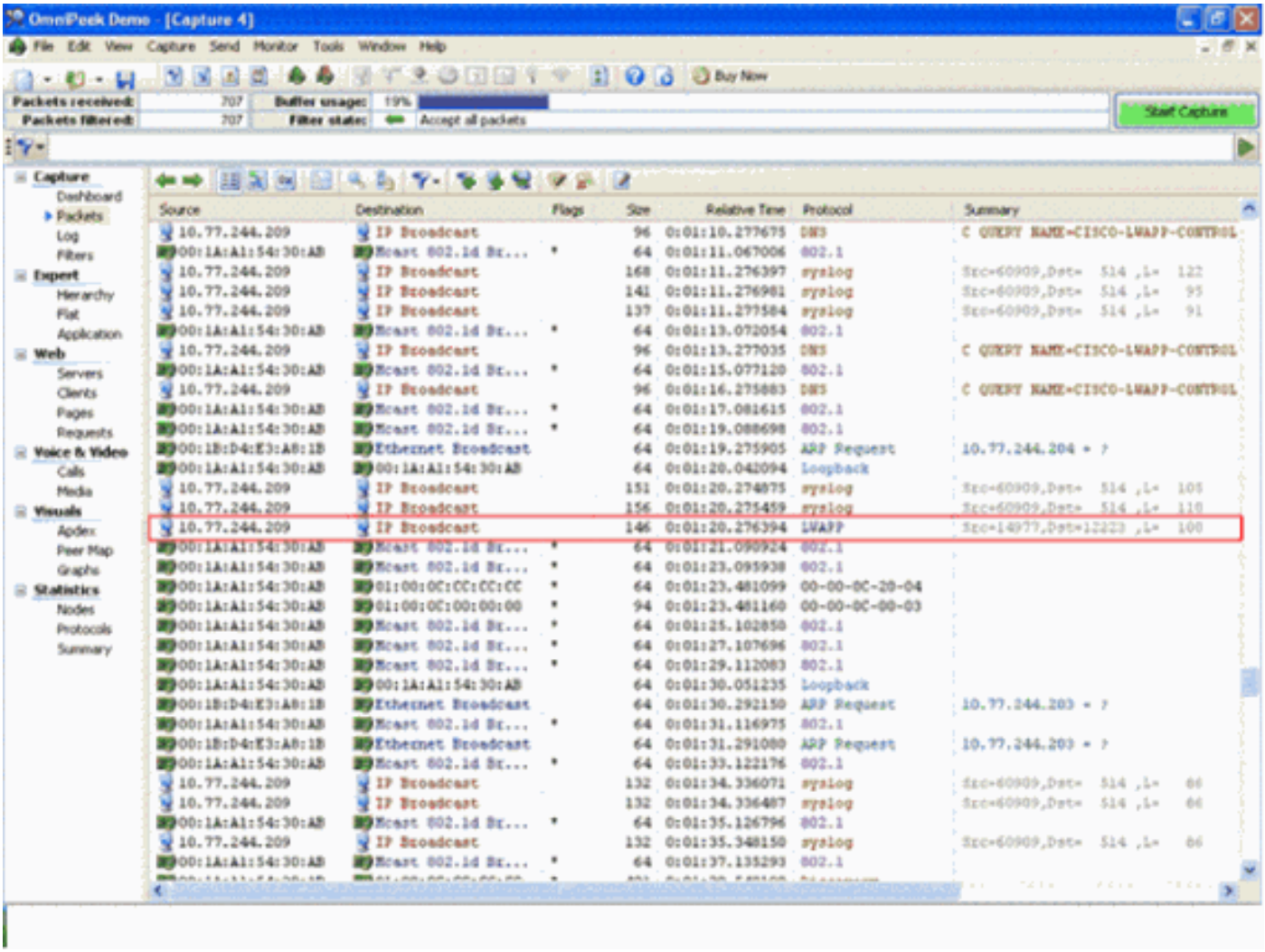
OmniPeek版本5.0是OmniPeek版本3.0的下一代捕獲工具。在5.0版本中，LWAPP解碼預設是內建的。因此，無需對檔案進行任何進一步更改。但是以下示例顯示如何使用IP地址和埠號在5.0版本中定義協定過濾器：

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。

驗證

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。圖1顯示LAP發出的發現請求期間的LWAPP協定捕獲。

圖1



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

- EtherPeek常見問題
- Omni簡介
- 下載OmniPeek 5.0
- 技術支援與文件 - Cisco Systems