在WildPackets OmniPeek和EtherPeek 3.0软件上的LWAPP解码实现

目录

简介
先决条件
要求
使用的组件
规则
修改LWAPP解码文件
修改TCP_UDP_Ports.dcd
修改Pspecs.xml文件
OmniPeek 5.0中的LWAPP解码
验证
相关信息

简介

WildPackets OmniPeek（和EtherPeek）提供轻量接入点协议(LWAPP)解码功能，但未插入。本文档说明如何启用LWAPP解码并使用软件查看LWAPP。本文档使用EtherPeek 3.0和OmniPeek 5.0的步骤。

注意：OmniPeek 3.0的步骤与EtherPeek 3.0的步骤相同。

注意：OmniPeek和EtherPeek软件之间的唯一区别是文件的位置。

- OmniPeek的路径是C:/Program Files/WildPackets/OmniPeek。
- EtherPeek的路径是C:/Program Files/WildPackets/EtherPeek。

先决条件

要求

思科建议您了解EtherPeek、OmniPeek 3.0和5.0软件。有关EtherPeek的信息，请参阅EtherPeek常见问题 。有关OmniPeek的信息，请参阅Omni简介 。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- OmniPeek 3.0

- EtherPeek 3.0
- OmniPeek 5.0

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

修改LWAPP解码文件

要修改LWAPP解码文件，请将“ETHR 0 0 90 c2 AP Identity: ; ”添加到LWAPP功能。这位于LWAPP-light_weight_...中的“LABL 0 0 0 b1轻量接入点协议\LWAPP: ; ”行下。protocol.dcd文件(C:\Program Files\WildPackets\EtherPeek\Decodes)。

修改TCP_UDP_Ports.dcd

在文件TCP_UDP_Ports.dcd(C:\Program Files\WildPackets\EtherPeek\Decodes)中，必须包括以下两行：

```
0x2fbe | LWAPP;
0x2fbf | LWAPP;
```

注意：由于此过程，主机计算机上没有打开任何端口。因此，此步骤不会使主机计算机面临任何安全风险。

这样，就包括了两个端口12222和12223。

修改Pspecs.xml文件

请完成以下步骤：

1. 在文件pspecs.xml(C:\Program Files\WildPackets\EtherPeek\1033)的用户数据报协议(UDP)部分，添加以下行：**注意：**确保先备份原始文件。

```
<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. 重新启动OmniPeek或EtherPeek，使更改生效。

OmniPeek 5.0中的LWAPP解码

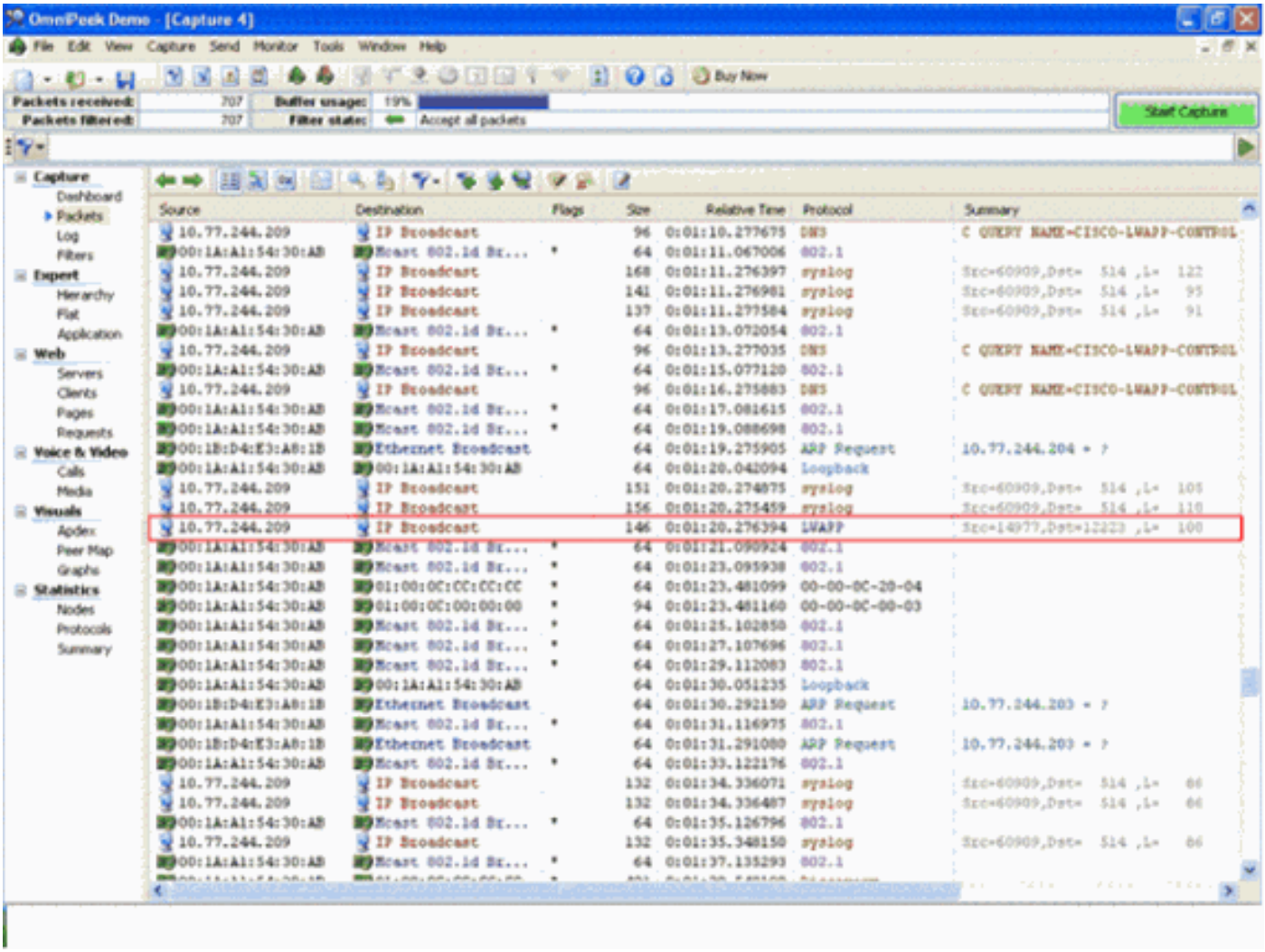
OmniPeek版本5.0是OmniPeek版本3.0的下一代捕获工具。在5.0版中，默认情况下会内置LWAPP解码。因此，文件中无需进一步更改。但是，以下示例显示如何使用IP地址和端口号在5.0版中定义协议过滤器：

1. 打开OmniPeek 5.0应用程序。
2. 在“开始”页中，单**击“文件”>**“新建”以打开“新建数据包捕获窗口”。系统将显示一个名为Capture Options的小窗口。它包含数据包捕获的选项列表。
3. 从“适配器”**选项**中，选择要使用该适配器捕获数据包的适配器。在突出显示适配器时，适配器的说明如下所示。选择**Local Area Connection**以使用本地以太网适配器捕获数据包。
4. Click **OK**.系统将显示New Capture窗口。
5. 单击“Start Capture(**开始捕获**)”按钮。该工具开始捕获软件中定义的协议的数据包。要查看捕获的数据包，请单击左侧**Capture**菜单下**的Packets选项。**
6. 右键单击捕获的任何数据包，然后单击**Make Filter**以定义新协议。系统将显示“插入过滤器”窗口。
7. 在过滤器框中输**入**名称以标识协议。启用地**址过**滤器。选择Type as IP以捕**获到**特定IP地址和从特定IP地址获取数据包。对于**Address1**，输入源IP地址。如果目**的地**址为静态IP，请在地址2中输入IP地址。如果目标通过DHCP**接收**IP地址，请选择Option作为Any Address。要指定数据包流的方向，请单击“Both directions”**按钮，**然后选择三个选项之一。按钮上的箭头标记表示选择的方向。启用端**口过**滤器。为协议使用的端口选择Type，例如TCP。对于端**口1**，输入源中使用的端口。如果目**标使**用标准的明确定义端口，请为端口2输入端口号。否则，如果目标**随机使**用某个端口，请选择“任意端口”选项。根据您*的*要求**，从“**两个方向”按钮选择方向。
8. 重复这些步骤以定义任何新的自定义协议。

验证

使用OmniPeek 5.0，您可以从Capture Screen中验证在触发LWAPP事件时，工具默认捕获LWAPP协议。图1显示了LAP在发现请求期间捕获的LWAPP协议。

图 1



双击该数据包，查看有关该数据包的详细信息。

相关信息

- EtherPeek常见问题
- 全向简介
- 下载OmniPeek 5.0
- 技术支持和文档 - Cisco Systems