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

目录

简介

WildPackets OmniPeek (和EtherPeek)有轻量级接入点协议(LWAPP)解码联机，但是他们没有接通。本文解释如何启用LWAPP解码并且使用软件查看LWAPP。本文使用步骤EtherPeek 3.0和OmniPeek 5.0。

注意： OmniPeek的3.0步骤是相同的象那EtherPeek 3.0。

注意： OmniPeek和EtherPeek软件之间的唯一的差异是文件的位置。

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

先决条件

要求

思科建议您有EtherPeek的知识和OmniPeek 3.0和5.0软件。关于EtherPeek的信息，参考EtherPeek FAQ 。关于OmniPeek的信息，参考介绍Omni 。

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

为了修改LWAPP解码文件，请添加“ETHR 0 0 90 c2 AP标识：; ”对LWAPP功能。这是直接地在“LABL下0 0 0 b1轻量级接入点协议\ LWAPP ：; ”在LWAPP-light_weight_… protocol.dcd文件(C:\Program Files\WildPackets\EtherPeek\Decodes)的线路。

修改TCP_UDP_Ports.dcd

在文件TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes)，您必须包括这两条线路：

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

注意： 由于此进程，端口在主机计算机没有打开。所以，此步骤不显示主机计算机在任何安全风险。

这样，两个端口12222和12223包括。

修改Pspecs.xml文件

完成这些步骤：

1. 在文件pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033)的用户数据报协议(UDP)部分，请添加这些线路：**注意：** 确保首先备份原始文件。
```
<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为了您的更改能生效。

在OmniPeek 5.0的LWAPP解码

OmniPeek版本5.0是OmniPeek版本3.0的下一代捕获工具。默认情况下在5.0版本中， LWAPP解码内藏。因此，没有任何更加另外的变化的需要在文件上。然而，这是使用IP地址和端口号，显示如何定义在5.0版本的协议过滤器的示例：

1. 打开OmniPeek 5.0应用程序。
2. 从一开始页，点击**新建的File>**为了打开新的数据包捕获窗口。名为捕获选项的一个小窗口出现。它包含选项列表数据包捕获的。
3. 使用该适配器，从**适配器选项**，请选择适配器获取数据包。当您突出显示适配器，关于适配器的说明如下所示。使用本地以太网适配器，选择**本地连接**获取数据包。
4. 单击 **Ok**。新的捕获窗口出现。
5. 点击**启动捕获**按钮。工具启动获取在软件里定义的协议的数据包。为了显示捕获的数据包，在左边的**捕获**菜单之下单击**数据包**选项。
6. 用鼠标右键单击捕获的其中任一数据包并且单击**做过滤器**为了定义一份新的协议。插入过滤器窗口出现。
7. 输入一名称在**过滤器**方框里面识别协议。启用**地址过滤器**。选择类型作为**IP**到/从特定IP地址获取数据包。对于**地址1请**输入源IP地址。对于**Address2，**如果目的地有一静态IP，请输入IP地址。如果目的地通过DHCP，收到IP地址请选择选项作为**所有地址**。为了指定数据包流单击的方向**两个方向**按钮和选择三个选项之一。在按钮的箭头马克指示选择的方向。启用**端口过滤器**。选择协议使用的端口的类型，例如TCP。用于来源的**Port1**回车端口。**端口2**回车端口编号，如果目的地使用一个标准的明确定义的端口。否则，如果目的地使用根据一个随机的基本类型的端口请选择**所有端口**选项。从根据您的需求的**两个方向**按钮选择*方向*。
8. 重复这些步骤定义其中任一新建的自定义协议。

验证

使用OmniPeek 5.0，您能从捕获屏幕验证工具捕获LWAPP协议默认情况下，当LWAPP事件被触发时。图1显示LWAPP协议捕获在LAP做的发现号请求期间。

图 1
在查看关于数据包的详细信息的数据包的双击。

相关信息

- EtherPeek FAQ
- 介绍Omni
- 下载OmniPeek 5.0
- 技术支持和文档 - Cisco Systems