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

#### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>修改LWAPP解码文件</u> <u>修改TCP\_UDP\_Ports.dcd</u> <u>修改Pspecs.xml文件</u> <u>OmniPeek 5.0中的LWAPP解码</u> <u>验证</u> 相关信息

## <u>简介</u>

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。

# <u>先决条件</u>

#### <u>要求</u>

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 <u>EtherPeek常见问题</u> 。有关OmniPeek的信息,请参阅<u>Omni简介</u> 。

#### <u>使用的组件</u>

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

#### <u>规则</u>

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)。

#### <u>修改TCP\_UDP\_Ports.dcd</u>

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。

## <u>修改Pspecs.xml文件</u>

请完成以下步骤:

 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>
```

2. 重新启动OmniPeek或EtherPeek,使更改生效。

## <u>OmniPeek 5.0中的LWAPP解码</u>

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。
- 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。

#### <u>验证</u>

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。<u>图1显</u>示了LAP在发现请求期间捕获的LWAPP协议。

图 1

ap rim EDK Vew	Capture Send Monitor Tool	s wedow help					
[ - 원 - 태 영제 최 승 유 영계 옷 이 다 1 위 회 중 중 by Now							
Packets received	207 Buffer usage: 19% Banding Banding						Contrast of the local division of the local
Packets filtered:	207 Filter s	tates 👄 Accept all packets					Sawe Capitan
19-							
= Capture	da an 100 51 621 53		10.00	12			
Deshboard				1.00	and the second	Reference in the second second	the second s
Packets	Source	Cestnation	riags	2624	Relative Tane	Protocol	Summary
Log	3 10.77.244.209	IP Buoadcast		96	0:01:10.277675	DW3	C OVERY NAME-CISCO-LWAPF-CONTROL
Fikers	#900:1A:A1:54:30:AB	BORDANE 802.14 BE	•	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 ,L= 122
Herarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	syslog	SIC+60909,D#t+ 514 ,L+ 95
Flat	3 10.77.244.209	IP Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t= 514 ,L= 91
Application	#900:1A:A1:54:30:AB	Boast 802.14 BE	•	64	0:01:13.072054	002.1	
😹 Web	10.77.244.209	🚼 IF Econdeast		96	0:01:13.277035	08/5	C QUERT NAME+CISCO-LWAPP-CONTROL
Servers	#900:1A:A1:54:30:A8	Bacast 802.14 Br		64	0:01:15.077120	802.1	
Clerits	10.77.244.209	IF Scondcast		96	0:01:16.275883	08/5	C OTERY NAME+CISCO-LWAPF-CONTROL
Pades	00:1A:A1:54:30:AB	#PRCast 802.14 St		64	0:01:17.081615	002.1	
Retainsts	B00:1A:A1:54:30:AB	Micast 802.1d Sr		64	0:01:19.088698	802.1	
Noice & Video	#900:18:D4:E3:A6:18	Ethernet Scondcast		64	0:01:19.275905	ARP Request	10.77.244.204 + 7
Call	2900:1A:A1:54:30:AB	00:1A:A1:54:30:A5		64	0:01:20.042094	Loopback	
Marka	10,77,244,209	IP Broadcast		151	0:01:20.274075	syslog	Src+60909.Det+ 514 .L4 105
C Microde	10,77,244,209	IP Broadcast		156	0:01:20.275459	syslog	Srca60909.Data 514 .Le 110
in visuals	10,77,244,209	I I Broadcast		146	0:01:20.276394	LVAPP	Src+14977.Dst+12223 .L+ 100
Page Mar	BERODY LALATE SAUSDIAN	MARANE 802.14 St		64	0:01:21.090924	607.1	
Peer Hap	BOOD 1 4 1 4 1 + 54 - 30 - 45	Rent 602.14 Br		64	0101123-095938	607-1	
tarapris .	BB00:11:41:54:30:48	B01+00+0C+CC+CC+CC		64	0101123.481099	00-00-00-20-04	
Statistics	100011A:A1:54:30:48	101-00-07-00-00-00			0-01-33 481140	00-00-00-00-00	
Nodes	BRODILLIA LISTING	Brance Boo Id Br			0108163-901109	442.1	
Protocols	POULARIALI SALSOLAD	ACASE OVER SEL	- C		0108165-202050	996-8	
Summary	APODI LAIALI S41 301AS	ACASE OVE.10 BE			0101127.107699	002-1	
	BOULATALIS41301AD	My Acast 002.1d BE	•	64	0101129-112083	494-1	
	0011A1A11541301AD	0011A1A11541301A5		64	0101130.051235	рооррася	
	#9001181D41£31A0118	By Ethernet Brosdrast	-	64	0:01:30.292150	The bedread	10.77.244.203 = 7
	#9-0011A1A11541301AB	B)Scent 002.1d Bc	•	64	0:01:31.116975	802.1	Lass and second
	#900:18:D4:E3:A8:18	#PEthernet Broadcast		64	0101131.291080	APP Pequest	10,77,244.203 = 2
	BOD:1A:A1:54:30:A8	BRCAST 802.14 St	•	64	0:01:33.122176	802.1	
	3 10.77.244.209	IP Buoadcast		132	0:01:34.336071	sysiog	fic-60909,Dst= 514 ,L= 66
	10.77.244.209	TP Broadcast		132	0:01:34.336487	#7#10g	Szc=60909,Dyt= 514 ,L= 66
	#900:1A:A1:54:30:AB	MCast 802.14 Br		64	0:01:35.126796	802.1	
	3 10.77.244.209	IF Scoadcast		132	0:01:35.348150	syslog	Src=60909,Dst= 514 ,L= 86
	00:1A:A1:54:30:AB	BCast 802.1d Br		64	0:01:37.135293	002.1	
	BRANCESS STREET					Ad	the set ware starting

双击该数据包,查看有关该数据包的详细信息。

# 相关信息

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