# O LWAPP decodifica a ativação em software WildPackets OmniPeek e EtherPeek 3.0

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Modificar o arquivo de decodificação LWAPP Modificar TCP\_UDP\_Ports.dcd Modificar o arquivo Pspecs.xml Decodificação LWAPP no OmniPeek 5.0 Verificar Informações Relacionadas

# **Introduction**

O WildPackets OmniPeek (e EtherPeek) tem decodificações Lightweight Access Point Protocol (LWAPP) disponíveis, mas não estão conectados. Este documento explica como habilitar os decodificadores do LWAPP e usar o software para examinar o LWAPP. Este documento usa o procedimento para EtherPeek 3.0 e OmniPeek 5.0.

Observação: o procedimento para o OmniPeek 3.0 é o mesmo do EtherPeek 3.0.

**Observação:** a única diferença entre os softwares OmniPeek e EtherPeek é a localização dos arquivos.

- O caminho para o OmniPeek é C:/Program Files/WildPackets/OmniPeek.
- O caminho para o EtherPeek é C:/Program Files/WildPackets/EtherPeek.

# **Prerequisites**

### **Requirements**

A Cisco recomenda que você tenha conhecimento dos softwares EtherPeek e OmniPeek 3.0 e 5.0. Para obter informações sobre o EtherPeek, consulte as <u>Perguntas Frequentes do EtherPeek</u>. Para obter informações sobre o OmniPeek, consulte <u>Introdução ao Omni</u>.

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

#### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

### Modificar o arquivo de decodificação LWAPP

Para modificar o arquivo de decodificação LWAPP, adicione "ETHR 0 90 c2 AP Identity:;" à função LWAPP. Isso está diretamente abaixo da linha "LABL 0 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" no LWAPP-light\_weight\_...arquivo protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

### Modificar TCP\_UDP\_Ports.dcd

No arquivo TCP\_UDP\_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), você deve incluir estas duas linhas:

0x2fbe | LWAPP; 0x2fbf | LWAPP;

**Observação:** nenhuma porta é aberta no computador como resultado desse processo. Portanto, esta etapa não expõe o computador host a riscos de segurança.

Dessa forma, as duas portas 12222 e 12223 estão incluídas.

# Modificar o arquivo Pspecs.xml

Conclua estes passos:

 Na seção User Datagram Protocol (UDP) do arquivo pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), adicione estas linhas:Nota: Certifique-se de fazer o backup do arquivo original primeiro.

```
<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. Reinicie o OmniPeek ou o EtherPeek para que as alterações entrem em vigor.

# Decodificação LWAPP no OmniPeek 5.0

O OmniPeek versão 5.0 é a ferramenta de captura de próxima geração para o OmniPeek versão 3.0. Na versão 5.0, os decodificadores LWAPP são incorporados por padrão. Assim, não há necessidade de mais alterações no arquivo. No entanto, aqui está um exemplo que mostra como definir um filtro de Protocolo na versão 5.0 usando um endereço IP e o número da porta:

- 1. Abra o aplicativo OmniPeek 5.0.
- Na página Iniciar, clique em Arquivo > Novo para abrir uma nova janela de captura de pacote.Uma pequena janela chamada Opções de captura é exibida. Contém a lista de opções para uma captura de pacote.
- 3. Na opção Adaptador, escolha um adaptador para Capturar pacotes usando esse adaptador. A descrição sobre o adaptador é mostrada abaixo quando você realça o adaptador. Escolha Conexão de Área Local para capturar pacotes usando o adaptador ethernet local.
- 4. Click OK.A janela Nova captura é exibida.
- 5. Clique no botão **Start Capture (Iniciar captura)**. A ferramenta começa a capturar pacotes para os protocolos definidos no software. Para visualizar os pacotes capturados, clique na opção **Pacotes** abaixo do menu **Captura** à esquerda.
- 6. Clique com o botão direito do mouse em qualquer pacote capturado e clique em **Make Filter** (Criar filtro) para definir um novo protocolo.A janela Inserir filtro é exibida.
- 7. Digite um nome dentro da caixa Filtro para identificar o protocolo. Ative o filtro de endereço. Escolha o Tipo como IP para capturar pacotes de e para endereços IP específicos. Para o Endereço1, insira o endereço IP de origem. Para o Endereço 2, insira um endereço IP se o destino tiver um IP estático. Escolha a Opção como Qualquer Endereço se o destino receber um endereço IP por meio do DHCP. Para especificar a direção do fluxo do pacote, clique no botão Ambas as direções e escolha uma das três opções. A marca de seta no botão indica a direção escolhida. Ative o filtro de porta. Escolha o Tipo para a porta usada pelo protocolo, por exemplo, TCP. Para a porta 1, insira uma porta usada na origem. Para a porta 2, insira um número de porta se o destino usar uma porta padrão bem definida. Caso contrário, escolha a opção Qualquer porta se o destino usar uma porta a porta a seu requisito.
- 8. Repita essas etapas para definir qualquer novo protocolo personalizado.

# **Verificar**

Com o OmniPeek 5.0, você pode verificar na tela Capture que a ferramenta captura o protocolo LWAPP por padrão quando um evento LWAPP é acionado. <u>A Figura 1</u> mostra a captura do protocolo LWAPP durante a solicitação de descoberta feita pelo LAP.

Fia	ure	1
I IM	ure	

File Edit View	Capture Send Monitor Took	s Wedow Help					and the second
) - () - 😡	3 3 6 3 4 4	8720001	9	0	👌 🕘 Buy Now		
ackets received:	707 Buffer un	aget 19%					But which it which it
Packets filtered:	707 Filter st	iatec 🗰 Accept all packets					- Copies
8-							
Capture	4 4 18 51 62 153		9.9	12	and the second second		
Deshboard	factor	Pederative	Elana -	- Cree	Relation Years	Restanted	Changes ( Story and Story and
Packets	310 22 244 200	a ra Breadaurt	rap		0-01-10.000/01	Protocol	C CONTRACT READER CONTRACT IN THE CONTRACT
Log	3 10.77.244.209	g 1F BEOBRCASE		20	0:01:10.277675	080	C DIERT NAME-CISCO-LWAPF-CONTROL
Fitters	POUL LATALISAT JULAS	MOAST 002.14 BE	•	04	0:01:11.067006	002.1	Law second and the second second
Expert	10.77.244.209	IF Broadcast		168	0:01:11.276397	sAsrod	SEC-60909,D#t= 514 ,L= 122
Hierarchy	10.77.244.209	IF Broadcast		141	0:01:11.276981	syslog	SIC+60909,D#5* 514 ,L* 95
Flat	3 10.77.244.209	IF Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t= 514 ,L= 91
Application	00:1A:A1:54:30:AB	. My Mcast 002.1d DE	•	64	0:01:13.072054	002.1	
Web	10.77.244.209	IP Broadcast		96	0:01:13.277035	08/5	C QUERT RAME+CISCO-LWAPP-CONTROL
Servers	#900:1A:A1:54:30:A8	Beast 802.14 Br	•	64	0:01:15.077120	802.1	
Clerits	3 10.77.244.209	🔮 IF Scoadcast		96	0:01:16.275883	D#/5	C QUERY NAME-CISCO-LWAPF-CONTROL
Pages	#900:1A:A1:54:30:AB	Mast 002.14 Br		64	0:01:17.081615	002.1	
Reparks	B001:1A:A1:54:30:AB	MpHcast 802.1d Sr		64	0:01:19.088698	802.1	
Voice & Video	#900:18:D4:E3:A8:18	Ethernet Scoadcast		64	0:01:19.275905	ARP Request	10.77.244.204 + 7
Calls	2900:1A:A1:54:30:AB	200:1A:AI:54:30:AB		64	0:01:20.042094	Loopback	
Marka	10.77.244.209	IP Broadcast		151	0:01:20.274075	syslog	SEC-60909,Det+ 514 ,L4 105
Minuals	10,77,244,209	IF Broadcast		156	0:01:20.275459	syslog	Sec+60909,Date 514 .L+ 110
Ander	10,77,244,209	12 Broadcast		1.46	0:01:20,276394	LVAPP	SEC+14977,Det+12223 .L= 100
Date Marc	20011A1A11541301A5	MCASE 802.18 St		64	0:01:21.090924	807.1	,
Combo	BOO: 14:41:54:30:48	BR(ast. 602.14 Br		64	0:01:23.095938	607-1	
Graphic .	BB00-14-41-54-30-48	B01+00+0C+CC+CC+CC		6.4	0101123.481099	00-00-00-20-04	
Statistics	\$\$00-11-11-54-30-18	201-00-07-00-00-00			0-01-23 481160	00-00-00-00-00	
Notes	200-11-11-11-54-30-120	Repar Bob 1d Br			0101125 102850	442 1	
Protocols	100011A1A11541301A0	White and the second	- C		0108167-202020	996-8	
Summary	APOULAIALIS41301AB	ACASE OVELED BELL			0104167-207099		
	By ODI LATALIS 41 JOLAS	My moast 002.14 St	•	64	0101129.112083	492-1	
	PODIIATA11541301AD	29 001 1A1 A11 541 301 A5		04	0101130.051235	рооррася	
	001181D41E31A0118	ByEthethet Brosdcast	-	64	0:01:30.292150	APP Request	10.77.244.203 = 7
	#POULTAIA11541301AB	My ACAST 002.14 St		64	0101131.116975	802.1	Los en este este este
	#900:18:D4:E3:A0:18	MyEthemet Broadcast		64	0:01:31.291080	ARP Request	10,77,244.203 = 7
	200:1A:A1:54:30:A8	BRCAST 802.14 St		64	0:01:33.122176	802.1	
	3 10.77.244.209	# IF Broadcast		132	0:01:34.336071	sysiog	fic-60909,Dst= 314 ,L= 66
	3 10.77.244.209	TP Broadcast		132	0:01:34.336407	#7#10g	Szc=60909,Dyt= 514 ,L= 66
	#200:1A:A1:54:30:AB	By Monast 002.14 Bg		64	0:01:35.126796	802.1	
	10.77.244.209	IP Buoadcast		132	0:01:35.348150	syslog	Src=60909,Dst= 514 ,L= 66
	#00:1A:A1:54:30:AB	BEAST 802.1d BE		64	0:01:37.135293	802.1	
	BRAN				PLATING PARLOS	And an and a second	

Clique duas vezes no pacote para ver os detalhes sobre o pacote.

# Informações Relacionadas

- Perguntas frequentes do EtherPeek
- Introdução ao Omni
- Download do OmniPeek 5.0
- Suporte Técnico e Documentação Cisco Systems