LWAPP Decodes Enable on Wild Packets Multimedia Peek en EtherPeek 3.0 Software

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Het LWAPP-decodebestand wijzigen TCP_UDP_Ports.dcd wijzigen Het bestand Pspecs.xml wijzigen LWAPP-decode in OmniPeek 5.0 Verifiëren Gerelateerde informatie

Inleiding

Wilde Packets OmniPeek (en EtherPeek) hebben lichtgewicht LWAPP-decoders (Access Point Protocol) beschikbaar, maar ze zijn niet aangesloten op de stekker. In dit document wordt uitgelegd hoe u de LWAPP-decoders kunt inschakelen en de software kunt gebruiken om naar LWAPP te kijken. Dit document gebruikt de procedure voor EtherPeek 3.0 en OmniPeek 5.0.

Opmerking: De procedure voor OmniPeek 3.0 is dezelfde als die voor EtherPeek 3.0.

Opmerking: het enige verschil tussen de software van OmniPeek en die van EtherPeek is de locatie van de bestanden.

- Het pad voor OmniPeek is C:/Program Files/WildPackets/OmniPeek.
- Het pad voor EtherPeek is C:/Program Files/WildPackets/EtherPeek.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de EtherPeek-software en de software van OmniPeek 3.0 en 5.0. Raadpleeg voor informatie over EtherPeek de <u>veelgestelde vragen</u> van <u>EtherPeek</u>. Raadpleeg voor informatie over OmniPeek de <u>Inleiding van Omni</u>.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Het LWAPP-decodebestand wijzigen

om het LWAPP-decodebestand te wijzigen, voegt u "ETHR 0 90 c2 AP Identity:" toe aan de LWAPP-functie. Dit staat direct onder "LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" lijn in de LWAPP-light_weight_...protocol.dcd-bestand (C:\Program Files\WildPackets\EtherPeek\Decodes).

TCP_UDP_Ports.dcd wijzigen

In het bestand TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes) moet u deze twee regels omvatten:

0x2fbe | LWAPP; 0x2fbf | LWAPP;

Opmerking: als gevolg van dit proces worden er geen poorten geopend op de host-computer. Daarom stelt deze stap de host-computer niet bloot aan beveiligingsrisico's.

Zo zijn de twee havens 12222 en 12223 opgenomen.

Het bestand Pspecs.xml wijzigen

Voer de volgende stappen uit:

 Voeg in het gedeelte User Datagram Protocol (UDP) van het bestand pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033) de volgende regels toe:N.B.: Zorg ervoor dat u eerst een back-up van het oorspronkelijke bestand maakt.

```
<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. Herstart OmniPeek of EtherPeek om uw wijzigingen in werking te laten treden.

LWAPP-decode in OmniPeek 5.0

OmniPeek versie 5.0 is het volgende generatie-opnamegereedschap voor OmniPeek versie 3.0. In de 5.0-versie worden LWAPP-decoders standaard ingebouwd. Het bestand hoeft dus niet verder te worden gewijzigd. Dit is echter een voorbeeld dat laat zien hoe u een protocolfilter in de 5.0-versie kunt definiëren met behulp van een IP-adres en het poortnummer:

- 1. Open de OmniPeek 5.0 applicatie.
- Klik vanuit de Start pagina op Bestand > Nieuw om een venster voor nieuwe pakketvastlegging te openen.Er verschijnt een klein venster met de naam Capture Opties. Het bevat de opties voor een pakketvastlegging.
- Kies in de optie Adapter een adapter om pakketten op te nemen met die adapter. De beschrijving van de adapter wordt hieronder weergegeven als u de adapter markeert. Kies Local Area Connection om pakketten op te nemen met behulp van de lokale Ethernetadapter.
- 4. Klik op OK.Het nieuwe Capture venster verschijnt.
- 5. Klik op de knop **Opname starten**.Het gereedschap begint pakketten op te nemen voor de protocollen die in de software zijn gedefinieerd. Klik op de optie **Packets** onder het menu **Opname** links om de opgenomen pakketten te bekijken.
- 6. Klik met de rechtermuisknop op een van de opgenomen pakketten en klik op **Filter maken** om een nieuw protocol te definiëren.Het venster Filter invoegen verschijnt.
- 7. Voer een naam in in het vakje Filter om het protocol te identificeren.Schakel het filter Adres in.Kies het type als IP om pakketten naar en van specifieke IP adressen op te nemen.Voer voor Adres1 het bron IP adres in.Voor Adres 2 ga een IP adres in als de bestemming een statische IP heeft.Kies de optie als elk adres als de bestemming een IP-adres via DHCP ontvangt.Om de richting van de pakketstroom in te stellen, klikt u op de knop Beide richtingen en vervolgens kiest u een van de drie opties. Het pijltje op de knop geeft de gekozen richting aan.Schakel het poortfilter in.Kies het type voor de poort die door het protocol wordt gebruikt, bijvoorbeeld TCP.Voor Port 1 voer u een poort in die in de bron wordt gebruikt.Voor Port 2 voer u een poortnummer in als de bestemming een standaard, duidelijk omschreven poort gebruikt.Kies anders de optie Elke poort als de bestemming een poort op willekeurige basis gebruikt.Kies een *richting* uit de knop Beide richtingen op basis van uw vereisten.
- 8. Herhaal deze stappen om een nieuw aangepast protocol te definiëren.

Verifiëren

Met OmniPeek 5.0 kunt u aan de hand van het Capture Screen controleren of het gereedschap standaard het LWAPP-protocol kan opnemen wanneer er een LWAPP-gebeurtenis wordt geactiveerd. <u>Afbeelding 1</u> toont de LWAPP-protocolopname tijdens het zoekverzoek van de LAP.

Figuur 1

ConniPeek Demi	o - [Capture 4]					a second a second second	
File Edit View	Capture Send Monitor Tool	s Wedow Help .					
🗟 - 😫 - 📮	💽 💽 🗈 🗶 🏘	8720001		: 0	Buy Now		
Packets received: 207 Buffer usage: 19%							Children of Antonio
Packets filtered:	207 🛛 Filter states 🗰 Accept al packets						Sale Capture
-							
= Capture	4 4 18 51 62 53		9.0	10			
Dashboard		Particular and an an	all and a	in the second	Relation Trees	Reference in the second	Parameter and the second
Packets	Source	Cesonacion	riags	3424	Reading Table	PTOROCON	Summery
Log	3 10.77.244.209	S 1F BEOBSCASE		90	0:01:10.277675	083	C OUEPT RATE-CISCO-LWAPF-CONTROL
Fitters	PODILATALIS47301AB	MCASE 002.14 BE	•	64	0:01:11.067006	002.1	A second second second second second
Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	sAsyod	SEC=60909,D#t= 514 ,L= 122
Herarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	sAsrod	SEC+60909,D#t+ 514 ,L+ 95
Flat	3 10.77.244.209	IF Broadcast		137	0:01:11.277584	sistod	SEC-60909,D9t= 514 ,L= 91
Application	00:1A:A1:54:30:AB	BOAST 002.14 BE	•	64	0:01:13.072054	002.1	
🗃 Web	10.77.244.209	IP Exceddest		96	0:01:13.277035	085	C QUERT HAME+CISCO-LWAPP-CONTROL
Servers	#900:1A:A1:54:30:A8	Beast 802.14 Br	•	64	0:01:15.077120	802.1	
Clerks	3 10.77.244.209	S IF Scondcast		96	0:01:16.275883	0個5	C QUERY NAME+CISCO-LWAPP-CONTROL
Pages	#900:1A:A1:54:30:AB	mast 002.14 Br		64	0:01:17.081615	002.1	
Reparks	B00:1A:A1:54:30:AB	Micast 002.1d Sr		64	0:01:19.088698	802.1	
Voice & Video	#900:18:D4:E3:A8:18	Ethernet Scondcast		64	0:01:19.275905	ARP Request	10.77.244.204 + /
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	Szc+60909,Det+ 514 ,L4 105
C Minuda	10,77,244,209	TP Broadcast		156	0:01:20.275459	syslog	Srca60909,Date 514 .Le 110
in visuals	10,77,244,209	12 Excadeast		1.46	0101120.276394	1.0499	\$rcal4977.bata12223 .Ls 100
Appen.	BRODI LALALI SAL SULAN	MARIAN DOT 14 Dr.		14	0(01)21.090924	807.1	
Peer Map	BOD-11-11-54-30-18	Wheet 607 1d Br			0103183-099924	607.1	
Graphs	2000114141154130140	10 AL ANA AR AR AR AR		64	0103187-077770	00-00-02-10-04	
Statistics	STOLIA CALLS SAL JULAD	01100100100100100		04	0101123,401099	00-00-00-00-00	
Nodes	490011A:A11541501A5	01100100100100100			0102123-402200	00-00-00-00	
Protocols	A 100 14141154130145	Macese 002.14 BE	- I	04	0101152-105620	401-1	
Summary	#90011A1A11541301A5	MyRcast 002.1d BE		64	0101127,107696	402-1	
	#90011A1A11541301AB	My Scast 002.1d St	•	64	0101129.112083	802-1	
	#900:1A:A1:54:30:A8	29 001 1A1 A11 541 301 A3		64	0:01:30.051235	Loopback	
	OD:18:D4:E3:A8:18	ByEthernet Broadcast		- 64	0:01:30.292150	ARP Request	10.77.244.203 = 7
	#90011A1A11541301AB	BBC685, 002.1d BC	*	64	0:01:31.116975	802.1	
	8900:18:D4:E3:A8:18	Ethemet Broadcast		64	0:01:31.291080	APP Request	10,77,244.203 = 2
	200:1A:A1:54:30:A8	Ecast 802.14 St		64	0:01:33.122176	802.1	
	3 10.77.244.209	IF Broadcast		132	0:01:34.336071	syslog	dzc-60909,Dat- 514 ,L- 66
	10.77.244.209	TP Broadcast		132	0:01:34.336487	syslog	Szc+60909,Dat= 514 ,1= 66
	#900:1A:A1:54:30:A8	BReast 802.14 Br		64	0:01:35.126796	802.1	
	10.77.244.209	IP Scoadcast		132	0:01:35,348150	syslog	Src+60909,Dat= 514 .L= 66
	#POD:14:41:54:30:45	BRANT 802.1d Br		64	0:01:37,135293	602.1	
				40.1	ALALIA FRANK	Ard 4 4 4 4 4 4 4 4	
	Concentration of the second						and the second second second

Dubbelklik op het pakket om de gegevens over het pakket te bekijken.

Gerelateerde informatie

- EtherPeek FAQ
- Inleiding Omni
- Downloadtoken 5.0
- <u>Technische ondersteuning en documentatie Cisco Systems</u>