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

Inhoud

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 veelgestelde vragen van EtherPeek . Raadpleeg voor informatie over OmniPeek de Inleiding van Omni .

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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor 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:

1. 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

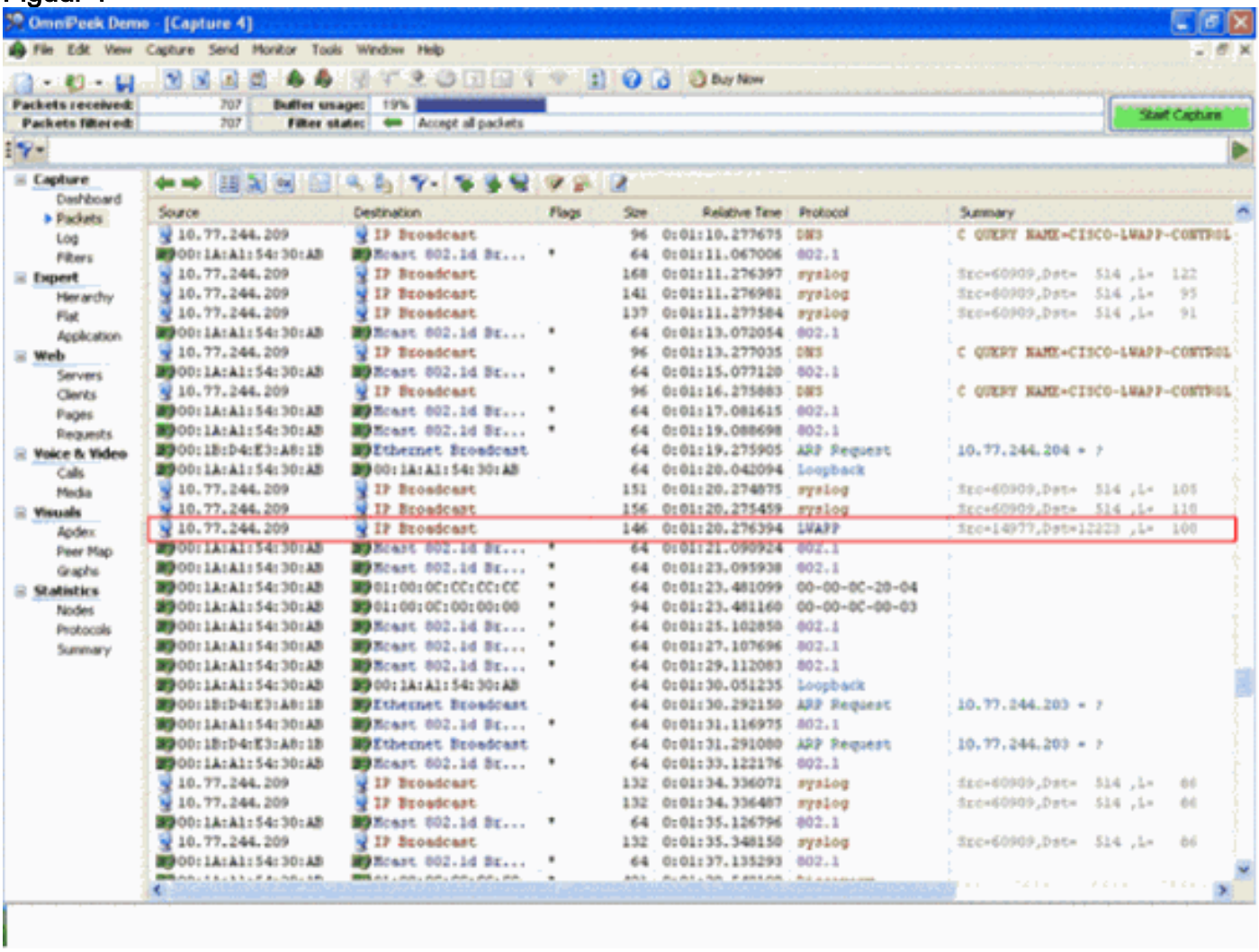
OmniPeek versie 5.0 is het volgende generatie-opnamegereedschap voor OmniPeek versie 3.0. In de 5.0-versie worden LWAPP-decoders standaard ingebouwd. Het bestand hoeft dus niet verder te worden gewijzigd. Dit is echter een voorbeeld dat laat zien hoe u een protocolfilter in de 5.0-versie kunt definiëren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

1. Open de OmniPeek 5.0 applicatie.
2. 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.
3. 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 Ethernet-adapter.
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. Afbeelding 1 toont de LWAPP-protocolopname tijdens het zoekverzoek van de LAP.

Figuur 1



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

Gerelateerde informatie

- EtherPeek FAQ
- Inleiding Omni
- Downloadtoken 5.0
- Technische ondersteuning en documentatie – Cisco Systems