LWAPP dekodiert Enablement für WildPackets OmniPeek- und EtherPeek 3.0-Software

Inhalt

Einführung

WildPackets OmniPeek (und EtherPeek) verfügen über LWAPP-Decodes (Lightweight Access Point Protocol), sind jedoch nicht angeschlossen. In diesem Dokument wird erläutert, wie Sie die LWAPP-Decodierung aktivieren und die Software zum Anzeigen von LWAPP verwenden. In diesem Dokument wird das Verfahren für EtherPeek 3.0 und OmniPeek 5.0 verwendet.

Hinweis: Das Verfahren für OmniPeek 3.0 ist mit dem von EtherPeek 3.0 identisch.

Hinweis: Der einzige Unterschied zwischen OmniPeek und EtherPeek ist der Speicherort der Dateien.

- Der Pfad für OmniPeek ist C:/Programme/WildPackets/OmniPeek.
- Der Pfad für EtherPeek ist C:/Programme/WildPackets/EtherPeek.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der Softwareprogramme EtherPeek und OmniPeek 3.0 und 5.0 zu verfügen. Weitere Informationen zu EtherPeek finden Sie in den EtherPeek-FAQ . Informationen zu OmniPeek finden Sie in Einführung von Omni .

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Ändern Sie die LWAPP-Decode-Datei.

Um die LWAPP-Dekodierungsdatei zu ändern, fügen Sie der LWAPP-Funktion "ETHR 0 90 c2 AP Identity:;" hinzu. Diese befindet sich direkt unter der Leitung "LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" in der Zeile LWAPP-light_weight_..protocol.dcd-Datei (C:\Program Files\WildPackets\EtherPeek\Decodes).

Ändern Sie TCP_UDP_Ports.dcd

In der Datei TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes) müssen die folgenden beiden Zeilen enthalten sein:

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

Hinweis: Durch diesen Prozess werden keine Ports auf dem Host-Computer geöffnet. Aus diesem Grund sind bei diesem Schritt keine Sicherheitsrisiken für den Host-Computer vorhanden.

Auf diese Weise sind die beiden Ports 1222 und 12223 enthalten.

Ändern Sie die Datei PSPT.XML

Gehen Sie wie folgt vor:

1. Fügen Sie im Abschnitt User Datagram Protocol (UDP) der Datei pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033) die folgenden Zeilen hinzu:**Hinweis:** Sichern Sie zuerst die Originaldatei.

```
<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. Starten Sie OmniPeek oder EtherPeek neu, damit Ihre Änderungen wirksam werden.

LWAPP-Decode in OmniPeek 5.0

OmniPeek Version 5.0 ist das Erfassungstool der nächsten Generation für OmniPeek Version 3.0. In der Version 5.0 sind die LWAPP-Decodes standardmäßig integriert. Daher sind keine weiteren Änderungen in der Datei erforderlich. Im folgenden Beispiel wird jedoch veranschaulicht, wie ein Protokollfilter in der Version 5.0 mithilfe einer IP-Adresse und der Portnummer definiert wird:

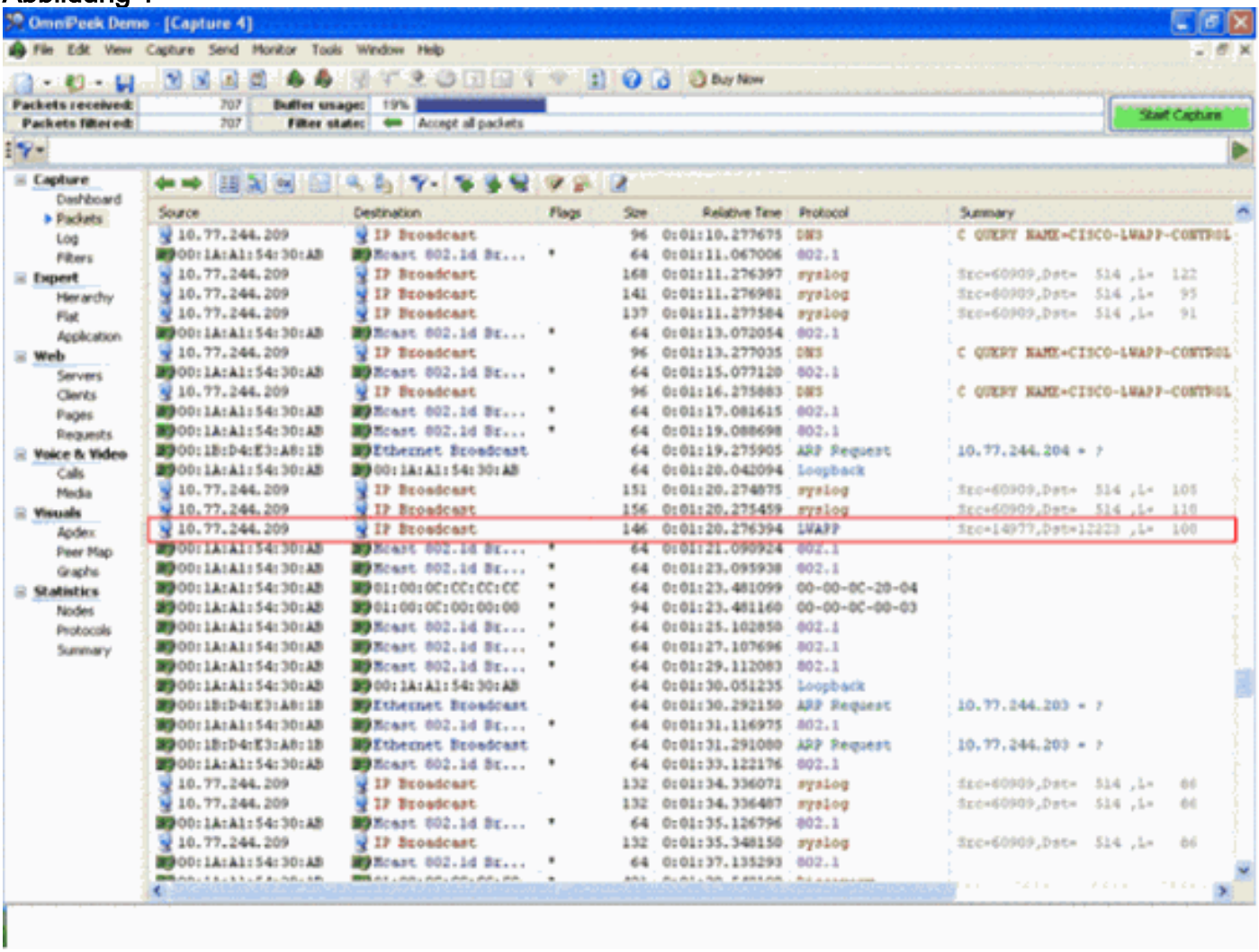
1. Öffnen Sie die Anwendung OmniPeek 5.0.
2. Klicken Sie auf der Startseite auf **Datei > Neu**, um ein Fenster zur Erfassung neuer Pakete zu öffnen.Ein kleines Fenster mit dem Namen Capture Options (Erfassungsoptionen) wird angezeigt. Sie enthält eine Liste von Optionen für die Paketerfassung.
3. Wählen Sie aus der **Adapter**-Option einen Adapter aus, um Pakete mit diesem Adapter zu erfassen. Die Beschreibung des Adapters wird unten angezeigt, während Sie den Adapter markieren. Wählen Sie **Local Area Connection** aus, um Pakete mit dem lokalen Ethernet-Adapter zu erfassen.
4. Klicken Sie auf **OK**.Das Fenster Neue Erfassung wird angezeigt.
5. Klicken Sie auf die Schaltfläche **Erfassung starten**.Das Tool erfasst Pakete für die in der Software definierten Protokolle. Um die erfassten Pakete anzuzeigen, klicken Sie auf die Option **Pakete** unter dem Menü **Erfassung** links.
6. Klicken Sie mit der rechten Maustaste auf eines der erfassten Pakete, und klicken Sie auf **Filter erstellen**, um ein neues Protokoll zu definieren.Das Fenster Filter einfügen wird angezeigt.
7. Geben Sie im Feld **Filter** einen Namen ein, um das Protokoll zu identifizieren.Aktivieren Sie den Adressfilter.Wählen Sie den Typ als **IP** aus, um Pakete zu und von bestimmten IP-Adressen zu erfassen.Geben Sie für die **Adresse1** die Quell-IP-Adresse ein.Geben Sie für die **Adresse 2** eine IP-Adresse ein, wenn das Ziel über eine statische IP-Adresse verfügt.Wählen Sie Option als **Any Address (Beliebige Adresse)** aus, wenn das Ziel über DHCP eine IP-Adresse erhält.Um die Richtung des Paketflusses anzugeben, klicken Sie auf die Schaltfläche **Both (Beide Richtungen)**, und wählen Sie eine der drei Optionen aus. Das Pfeilsymbol auf der Schaltfläche gibt die gewählte Richtung an.Aktivieren Sie den **Port-**Filter.Wählen Sie den Typ für den vom Protokoll verwendeten Port aus, z. B. TCP.Geben Sie für **Port 1** einen Port ein, der in der Quelle verwendet wird.Geben Sie für **Port 2** eine Portnummer ein, wenn für das Ziel ein gut definierter Standardport verwendet wird.Andernfalls wählen Sie die Option **Any port** (Beliebiger Port), wenn das Ziel einen zufälligen Port verwendet.Wählen Sie eine *Richtung* aus der Schaltfläche **Both Directions** (**Beide Richtungen**).

8. Wiederholen Sie diese Schritte, um ein neues benutzerdefiniertes Protokoll zu definieren.

Überprüfen

Mit OmniPeek 5.0 können Sie im Erfassungsbildschirm überprüfen, ob das Tool standardmäßig das LWAPP-Protokoll erfasst, wenn ein LWAPP-Ereignis ausgelöst wird. Abbildung 1 zeigt die LWAPP-Protokollerfassung während der von der LAP durchgeführten Erkennungsanfrage.

Abbildung 1



Doppelklicken Sie auf das Paket, um die Details zum Paket anzuzeigen.

Zugehörige Informationen

- EtherPeek-FAQ
- Einführung von Omni
- OmniPeek 5.0 herunterladen
- Technischer Support und Dokumentation - Cisco Systems