Activation du décodage LWAPP sur les logiciels WildPackets OmniPeek et EtherPeek 3.0

Contenu

Introduction

WildPackets OmniPeek (et EtherPeek) ont des décodes LWAPP (Lightweight Access Point Protocol) disponibles, mais ils ne sont pas branchés. Ce document explique comment activer les décodes LWAPP et utiliser le logiciel pour examiner LWAPP. Ce document utilise la procédure pour EtherPeek 3.0 et OmniPeek 5.0.

Remarque : La procédure pour OmniPeek 3.0 est identique à celle d'EtherPeek 3.0.

Note : La seule différence entre les logiciels OmniPeek et EtherPeek est l'emplacement des fichiers.

- Le chemin pour OmniPeek est C:/Program Files/WildPackets/OmniPeek.
- Le chemin pour EtherPeek est C:/Program Files/WildPackets/EtherPeek.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les logiciels EtherPeek et OmniPeek 3.0 et 5.0. Pour plus d'informations sur EtherPeek, consultez la FAQ EtherPeek. Pour plus d'informations sur OmniPeek, référez-vous à Présentation d'Omni .

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Modifier le fichier de décodage LWAPP

Afin de modifier le fichier de décodage LWAPP, ajoutez « ETHR 0 0 90 c2 AP Identity:; » à la fonction LWAPP. Ceci est directement sous la ligne « LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:; » dans la ligne LWAPP-light_weight_..protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modifier TCP_UDP_Ports.dcd

Dans le fichier TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), vous devez inclure les deux lignes suivantes :

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

Remarque : Aucun port n'est ouvert sur l'ordinateur hôte à la suite de ce processus. Par conséquent, cette étape n’expose pas l’ordinateur hôte à des risques de sécurité.

Les deux ports 12222 et 1223 sont ainsi inclus.

Modifier le fichier Pspecs.xml

Procédez comme suit :

1. Dans la section User Datagram Protocol (UDP) du fichier pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), ajoutez les lignes suivantes :**Remarque :** Veillez à sauvegarder d'abord le fichier d'origine.

```
<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. Redémarrez OmniPeek ou EtherPeek afin que vos modifications prennent effet.

Décodage LWAPP dans OmniPeek 5.0

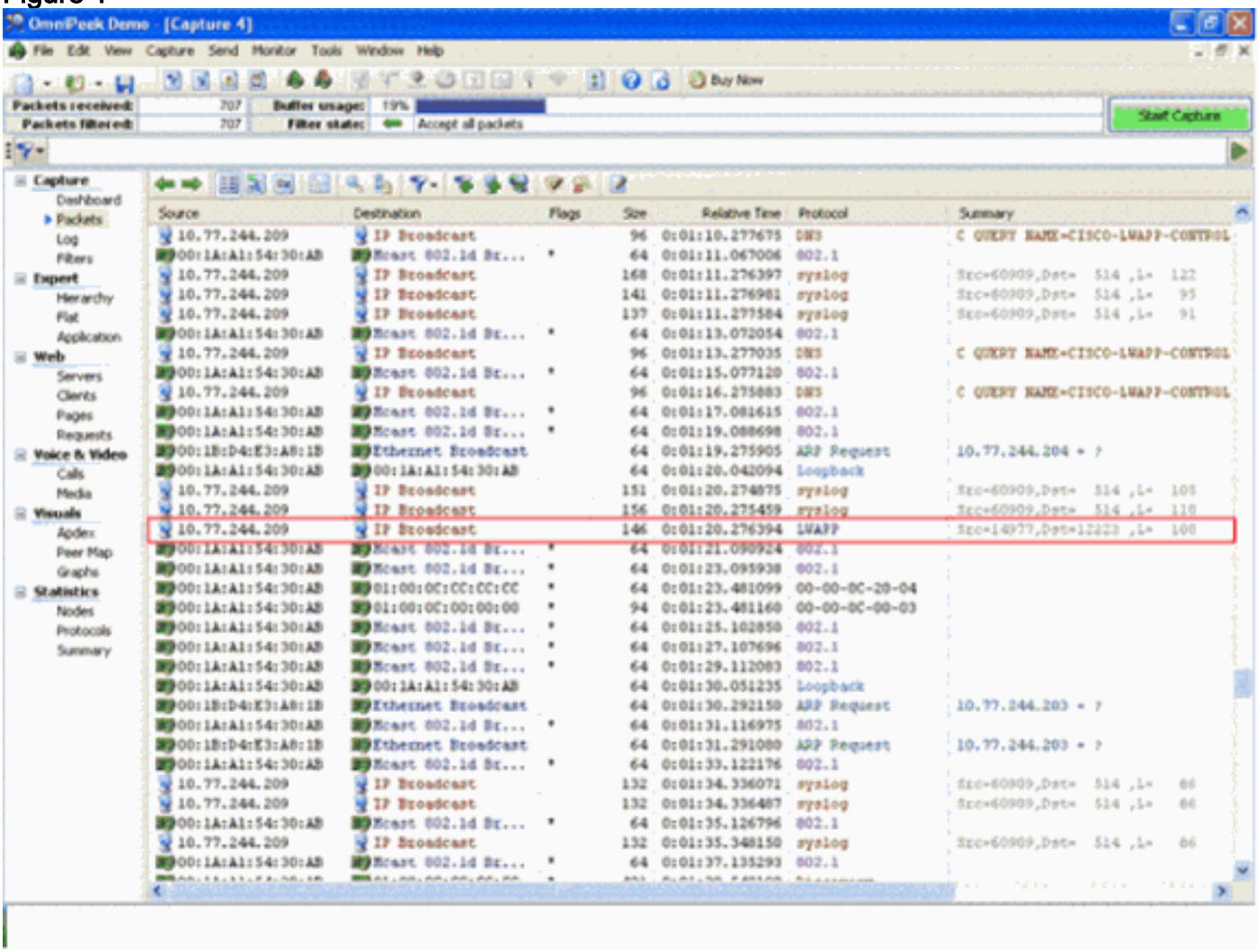
OmniPeek version 5.0 est l'outil de capture de nouvelle génération pour OmniPeek version 3.0. Dans la version 5.0, les décodes LWAPP sont intégrés par défaut. Par conséquent, il n'est pas nécessaire d'apporter d'autres modifications au fichier. Cependant, voici un exemple qui montre comment définir un filtre de protocole dans la version 5.0 à l'aide d'une adresse IP et du numéro de port :

1. Ouvrez l'application OmniPeek 5.0.
2. Dans la page Démarrer, cliquez sur **Fichier > Nouveau** afin d'ouvrir une nouvelle fenêtre de capture de paquets.Une petite fenêtre intitulée Options de capture apparaît. Il contient la liste des options pour une capture de paquets.
3. Dans l'option **Adaptateur**, sélectionnez une carte pour capturer des paquets à l'aide de cette carte. La description de l'adaptateur s'affiche ci-dessous lorsque vous mettez l'adaptateur en surbrillance. Choisissez **Connexion au réseau local** pour capturer les paquets à l'aide de la carte Ethernet locale.
4. Click OK.La fenêtre Nouvelle capture apparaît.
5. Cliquez sur le bouton **Start Capture**.L'outil commence à capturer des paquets pour les protocoles définis dans le logiciel. Afin d'afficher les paquets capturés, cliquez sur l'option **Packets** sous le menu **Capture** à gauche.
6. Cliquez avec le bouton droit sur l'un des paquets capturés et cliquez sur **Make Filter** afin de définir un nouveau protocole.La fenêtre Insérer un filtre apparaît.
7. Entrez un nom dans la zone **Filtre** pour identifier le protocole.Activez le filtre **Adresse**.Choisissez le type en tant qu'**IP** pour capturer les paquets à destination et en provenance d'adresses IP spécifiques.Pour l'**adresse 1**, saisissez l'adresse IP source.Pour l'**adresse 2**, saisissez une adresse IP si la destination a une adresse IP statique.Sélectionnez l'option **Any Address** si la destination reçoit une adresse IP via DHCP.Afin de spécifier la direction du flux de paquets, cliquez sur le bouton **Les deux directions** et choisissez l'une des trois options. La flèche du bouton indique la direction choisie.Activez le filtre **Port**.Sélectionnez le type du port utilisé par le protocole, par exemple TCP.Pour le **port 1**, saisissez un port utilisé dans la source.Pour le **port 2**, saisissez un numéro de port si la destination utilise un port standard bien défini.Sinon, choisissez l'option **N'importe quel port** si la destination utilise un port de manière aléatoire.Choisissez une *direction* à partir du bouton **Deux directions** en fonction de vos besoins.
8. Répétez ces étapes pour définir un nouveau protocole personnalisé.

Vérification

Avec OmniPeek 5.0, vous pouvez vérifier à partir de l'écran Capture que l'outil capture le protocole LWAPP par défaut lorsqu'un événement LWAPP est déclenché. La Figure 1 montre la capture du protocole LWAPP lors de la requête de découverte effectuée par le LAP.

Figure 1



Double-cliquez sur le paquet pour afficher les détails du paquet.

Informations connexes

- FAQ EtherPeek
- Présentation de Omni
- Télécharger OmniPeek 5.0
- Support et documentation techniques - Cisco Systems